The Dissertation Committee for Leslie Danielle Hayes
Certifies that this is the approved version of the following dissertation:

THE PLUS CLOSURE OF AN IDEAL

Committee:

Raymond C. Heitmann, Supervisor

Daniel Katz

Stephen J. McAdam

David J. Saltman

Felipe Voloch

THE PLUS CLOSURE OF AN IDEAL

by

LESLIE DANIELLE HAYES, B.A., M.S.

DISSERTATION

Presented to the Faculty of the Graduate School of

The University of Texas at Austin

in Partial Fulfillment

of the Requirements

for the Degree of

DOCTOR OF PHILOSOPHY

THE UNIVERSITY OF TEXAS AT AUSTIN

August 2001

For David

Acknowledgments

I am most grateful to Ray Heitmann for his many helpful comments which made this thesis possible as well as for his exceptional advising over the past four years. I feel lucky to have had the opportunity to work with him and I can't imagine a better advisor.

Part of this work was done with the support of a NSF grant from Karen Uhlenbeck whom I would like to thank for that help. She and the many strong, intelligent, extremely supportive women whom I have known while at UT-Austin (Angela, Cynthia, Dorothy, Katherine, Melissa, and many others) made this a wonderful place to be a female student of mathematics.

I would like to thank my family for their love and support over the years. My parents gave me the educational opportunities they never had; words cannot express my gratitude for that. They and my sisters Lynnae and Lisann are an inspiration to me. I am also grateful to Sherry and J. Weiland who have been like a second set of parents.

To David, who has brightened every one of my days since we met, I am particularly indebted.

THE PLUS CLOSURE OF AN IDEAL

Publication No. _____

Leslie Danielle Hayes, Ph.D.
The University of Texas at Austin, 2001

Supervisor: Raymond C. Heitmann

If R is a local integral domain let R^+ denote the integral closure of R in an algebraic closure of its quotient field. If $z \in R^+$ we would like to understand the conditions under which $z \in IR^+$, where I is an ideal of R. Necessary and sufficient conditions on the coefficients of the minimal irreducible polynomial for z are known when I is generated by two elements of a regular system of parameters and when z is in a degree two extension of R. In this thesis we obtain results for the case when $z^3 \in R$, as well as a sufficient condition for z to be in IR^+ when $z^a \in R$ for $a \geq 1$ and when I has a finite number of generators.

Table of Contents

Acknowledgments **v**

Abstract **vi**

Chapter 1. Introduction **1**

Chapter 2. Preliminary Results **4**

Chapter 3. Sufficient Conditions **14**

Chapter 4. Necessary Conditions **33**

Bibliography **58**

Vita **59**

Chapter 1

Introduction

Let R be an integral domain and I an ideal of R. The plus closure of I, denoted I^+, is defined to be $IR^+ \cap R$, where R^+ is the integral closure of R in an algebraic closure of its quotient field. Since $I^+ = \cap(IR_P)^+$ [1, p. 691] where the intersection is taken over all prime ideals P, we may restrict our attention to local integral domains, of which there are three types: those which contain the rationals (equicharacteristic 0), those which contain finite fields (equicharacteristic p), and those which do not contain a field (mixed characteristic).

If R is integrally closed and contains the rationals, then it is well known that $IS \cap R = I$ for any integral extension S of R. [This is easy to prove using a trace argument]. Hence $I^+ = I$.

In the equicharacteristic p case, $I^+ \subseteq I^*$, where I^* denotes the tight closure of I, and it is conjectured that equality holds. As noted above, the plus closure is a local property, so understanding it may help solve the primary problem in tight closure theory: does $I = I^*$ imply that $I_P = I_P^*$ for all prime ideals P?

In the mixed characteristic case, little is known about the plus closure.

A 30-year old conjecture known as the monomial conjecture is actually an assertion that certain elements are not in the plus closures of certain ideals in regular local rings. Understanding the plus closure would also allow us to determine if R^+ is Cohen-Macaulay in dimension 3. If this is in fact the case, a number of conjectures could be proven.

The question on which we will focus is the following: if I is an ideal in a regular local ring R and $z \in R^+$, when is $z \in IR^+$? Heitmann [2] has answered this question in the case where z satisfies a degree two polynomial $f(T) = T^2 + c_1T + c_2$ over R and $I = (x, y)R$, where x, y are part of a regular system of parameters for R. Letting $\Delta = (c_1)^2 - 4c_2$ denote the discriminant of f, his main result is the following:

Theorem 1.1. *Let R be a regular local ring, x, y part of a regular system of parameters, and $p \in (x, y)R$ with $p > 5$. Then $z \in IR^+$ if and only if $c_1 \in I$ and either (1) $\Delta \in t^2R$ for some $t \in I$, (2) $\Delta \in I^4$, or (3) $\Delta \in (t, I^2)^3R$ for some $t \in I$.*

Notice that if $z^2 \in R$, then (1), (2), and (3) become $z^2 \in t^2R$, $z^2 \in I^4$, and $z^2 \in (t, I^2)^3R$ respectively. If $z^3 \in R$, we make the following conjecture:

Conjecture 1.2. *Let R be a regular local ring and let x, y be part of a regular system of parameters for R. Suppose that p is a sufficiently large prime number*

and $p \in I = (x, y)R$. Let $z \in R^+$ such that $z^3 \in R$. Then $z \in IR^+$ if and only if one of the following holds:

(1) $z^3 \in t^3R$ *for some* $t \in I$

(2) $z^3 \in I^6$

(3) $z^3 \in (t, I^3)^4$ *for some* $t \in I$

(4) $z^3 \in (t, I^2)^5$ *for some* $t \in I$

(5) $z^3 \in (t^5, I^8)$ *for some* $t \in I$.

The reverse implication is given as Corollary 3.14 in Chapter 3. The progress made toward the forward direction is discussed in Chapter 4. In particular, Proposition 4.8 shows that if (1) does not hold, then $z^3 \in t^4R + I^5R$ for some $t \in I$. Theorem 4.9 and Theorem 4.15 then eliminate most of the remaining cases when $z^3 \notin I^5$.

In Chapter 3 we also prove the following result which holds for $z^a \in R$, $a \geq 1$, and for an ideal I having a finite number of generators.

Corollary 1.3. *Let R be an integrally closed integral domain and $I = (x_1, \ldots, x_{k+1})$ an ideal with $p \in \sqrt{I}$. Suppose $a, b_1, \ldots, b_k, c, d$ are positive integers such that $c > b_1$, and $t_1, \ldots, t_k \in I$ with $z^a \in (t_1^{b_1}, \ldots, t_k^{b_k}, I^c)^d$ where $\frac{1}{b_1} + \cdots + \frac{1}{b_k} + \frac{k}{c} \leq \frac{d}{a}$. Then $z \in IR^+$.*

Chapter 2

Preliminary Results

All rings are assumed to be integral domains. Throughout this paper, $\lfloor x \rfloor$ will denote the greatest integer less than or equal to x. In Lemma 4.11, we will also have need of $\lceil x \rceil$, which denotes the least integer greater than or equal to x. We begin by recalling the definition of the plus closure.

Definition 2.1. Let R be an integral domain and let I be an ideal of R. Then the plus closure of I, denoted I^+, equals $IR^+ \cap R$ where R^+ denotes the integral closure of R in an algebraic closure of its quotient field.

The following lemma (Lemma 1.1 of [1]) shows that in studying the plus closure we may restrict our attention to local domains.

Lemma 2.1. *Let R be an integral domain and let I be an ideal of R. Then $I^+ = \cap (IR_P)^+$ where the intersection may be taken either over all prime ideals P or all maximal ideals P.*

In what follows p will denote the characteristic of the residue field of any local ring under consideration as well as the ring element $p \cdot 1$.

If $z \in (x,y)R^+$, say $z = yv + xw$ for some elements $v, w \in R^+$, then the minimal polynomial which w satisfies over R determines the minimal polynomial for v. More precisely, we have the following lemma from [1]:

Lemma 2.2. *Let $f(T) = \sum_{i=0}^{n} a_i T^{n-i}$ be a monic polynomial and suppose $f(w) = 0$. For $0 \leq i \leq n$, set $b_i = (-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j z^{i-j}$ and let $g(T) = \sum_{i=0}^{n} b_i T^{n-i}$. Then $g(z - xw) = 0$.*

Proof. Set $h(T) = \sum_{i=0}^{n} a_i x^i T^{n-i}$. Then $h(xw) = x^n f(w) = 0$. Next expand $h(T)$ as a Taylor polynomial in $T - z$. Thus $h(T) = \sum_{i=0}^{n} c_i (T-z)^{n-i}$ with $c_i = h^{n-i}(z)/(n-i)!$. We claim $c_i = \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j z^{i-j}$. The claim is easily checked by induction on $n-i$. For $i = n$, it is clear. Assuming $c_i = \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j z^{i-j}$ for some value of i, we compute c_{i-1} by taking the derivative with respect to z and dividing by $n+1-i$. Since $\binom{n-j}{i-j}((i-j)/(n+1-i)) = \binom{n-j}{i--1-j}$, $c_{i-1} = \sum j = 0i-1 \binom{n-j}{i-1-j} a_j x^j z^{i-j-1}$ as desired. Now $0 = h(xw) = \sum_{i=0}^{n} c_i (xw - z)^{n-i}$ and since $b_i = (-1)^i c_i$, $g(z - xw) = 0$. □

We would like to have a monic polynomial $G(T)$ such that $G(\frac{z-xw}{y}) = 0$. With the notation of lemma 2.2, suppose that $b_i \in y^i R$, say $b_i = y^i B_i$. Let

$G(T) = \sum B_i T^{n-i}$. Then G is monic and

$$\begin{aligned} G(\frac{z-xw}{y}) &= \sum_{i=0}^{n} B_i y^{i-n}(z-xw)^{n-i} \\ &= y^{-n}\sum_{i=0}^{n} b_i(z-xw)^{n-i} \\ &= 0. \end{aligned}$$

We have now proven:

Lemma 2.3. *Let $x, y, z \in R$ and let $I = (x, y)R$. If $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ are integral over R and for $0 \leq i \leq n$,*

$$\sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j z^{i-j} = b_i y^i,$$

then $z \in IR^+$.

We also recall the definition of the integral closure of an ideal.

Definition 2.2. Let I be an ideal of R. Then $z \in R$ is defined to be in the integral closure of I, denoted $\overline{I}$, if there exists a monic polynomial $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ such that $f(z) = 0$ and each $a_i \in I^i$.

Note that $z \in \overline{I}$ if and only if $z^n \in I(I, z)^{n-1}$ for some n.

In Chapter 3 we will make use of the extended Rees ring of R with respect to an ideal I.

Definition 2.3. Let R be a ring and I an ideal of R. The extended Rees ring of R with respect to I is the ring $R[It, u]$ where t is an indeterminate and $u = t^{-1}$.

The ring $R[It, u]$ has a natural $\mathbb{Z}$-grading: let R be the homogeneous summand of degree zero and assign $\deg(t) = 1$. Let S denote the integral closure of $R[It, u]$. Then S is also a $\mathbb{Z}$-graded ring and for $n > 0$ the degree n summand is $\overline{I^n}t^n$. An important consequence is that the intersection of the ideal $(u^n)S$ with the degree zero summand is equal to the integral closure of I^n in R. Hence the extended Rees ring provides a way to reduce problems about finitely generated ideals to problems about principal ideals.

When dealing with integral extensions of graded rings, we will restrict our attention to those extensions which respect the grading in the sense of the next definition.

Definition 2.4. An integral extension S of R is called a g-integral extension if R is a graded subring of S.

Since any ring can be given the trivial grading, any integral extension of non-graded rings can be thought of as a g-integral extension.

In Chapter 3 we'll need some facts about the discriminant of a polynomial.

Definition 2.5. Let $f(T) = (T - \sigma_1) \cdots (T - \sigma_n)$. Then the discriminant of f is defined to be $\Delta_f = \prod_{i<j} (\sigma_i - \sigma_j)^2$.

It is easy to see that the discriminant is a symmetric polynomial and homogeneous of degree $2\binom{n}{2} = n(n-1)$ in $\sigma_1, \ldots, \sigma_n$. For a monomial $X_1^{\alpha_1} \cdots X_n^{\alpha_n}$ in the variables $X_1, \ldots, X_n$, define the weight of the monomial to be $\alpha_1 + 2\alpha_2 + \cdots + n\alpha_n$. Let $a_1, \ldots, a_n$ be the elementary symmetric polynomials of $\sigma_1, \ldots, \sigma_n$. So, for example, $a_1 = \sigma_1 + \cdots + \sigma_n$ and $a_n = \sigma_1 \cdots \sigma_n$. The next theorem is a slight variation of Theorem 6.1 of [4, p. 191].

Theorem 2.4. *Let $f(\sigma) \in R[\sigma_1, \ldots, \sigma_n]$ be symmetric and homogeneous of degree d. Then there exists a polynomial $g(X_1, \ldots, X_n)$, every term of which has weight d, such that $f(\sigma) = g(a_1, \ldots, a_n)$.*

Proof. We induct on n. The theorem is obvious if $n = 1$ since $a_1 = \sigma_1$. Assume the result is true for polynomials in $n - 1$ variables.

We now induct on d. If $d = 0$, the assertion is trivial. Assume $d > 0$, and assume the result is true for polynomials homogeneous of degree $< d$. Let $f(\sigma_1, \ldots, \sigma_n)$ be homogeneous of degree d. There exists a polynomial $g_1(X_1, \ldots, X_{n-1})$, every term of which has weight d, such that

$$f(\sigma_1, \ldots, \sigma_{n-1}, 0) = g_1(a'_1, \ldots, a'_{n-1}),$$

where $a'_1, \ldots, a'_{n-1}$ are the elementary symmetric polynomials of $\sigma_1, \ldots, \sigma_{n-1}$. We note that $g_1(a_1, \ldots, a_{n-1})$ is homogeneous of degree d in $\sigma_1, \ldots, \sigma_n$. The polynomial

$$f_1(\sigma_1, \ldots, \sigma_n) = f(\sigma_1, \ldots, \sigma_n) - g_1(a_1, \ldots, a_{n-1})$$

is homogeneous of degree d (in $\sigma_1, \ldots, \sigma_n$) and is symmetric. We have

$$f_1(\sigma_1, \ldots, \sigma_{n-1}, 0) = 0.$$

Hence f_1 is divisible by σ_n, i.e. contains σ_n as a factor. Since f_1 is symmetric, it contains $\sigma_1 \cdots \sigma_n$ as a factor. Hence

$$f_1(\sigma_1, \ldots, \sigma_n) = a_n f_2(\sigma_1, \ldots, \sigma_n)$$

for some polynomial f_2, which must be symmetric and homogeneous of degree $d - n$. By induction, there exists a polynomial g_2 in n variables each term of which has weight $d - n$ such that

$$f_2(\sigma_1, \ldots, \sigma_n) = g_2(a_1, \ldots, a_n).$$

We obtain

$$f(\sigma) = g_1(a_1, \ldots, a_{n-1}) + a_n g_2(a_1, \ldots, a_n),$$

and each term on the right has weight d, which proves the theorem. □

Hence if $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$, then Δ_f can be expressed as a polynomial in $a_1, \ldots, a_n$. In fact, we have the following:

Proposition 2.5. *Let $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$. Then as a function of $a_1, \ldots, a_n$, the discriminant $\Delta_f = N(a_{n-1})^n$+lower degree terms in a_{n-1}, where N is an integer which is a unit if $p \not| (n-1)$.*

First we need the following lemma.

Lemma 2.6. *If $f(T) = T^n - 1$, then Δ_f is a unit unless $p \mid n$.*

Proof. We know that Δ_f is an integer. Also, it follows from the definition of the discriminant that Δ_f is contained in some prime ideal P if and only if $\sigma_i - \sigma_j \in P$ for two roots σ_i, σ_j of f. This happens if and only if $f(T)$ and $f'(T)$ have a common root modulo P. This occurs if and only if n is in P. Hence, if n is a unit, so is Δ_f. □

Proof of Proposition 2.5. Since the degree of Δ_f is $n(n-1)$, by Theorem 2.4 we may write $\Delta_f = g(a_1, \ldots, a_n)$ for some polynomial g, every term of which has weight $n(n-1)$. Hence as a function of a_n, $\Delta_f = N_0(a_{n-1})^n + N_1(a_{n-1})^{n-1} + \cdots + N_n$, where $N_1, \ldots, N_n$ are non-constant functions of $a_1, \ldots, a_{n-2}, a_n$ and N_0 is a constant.

Now, $g(0, \ldots, 0, -1, 0) = \pm N_0$ =the discriminant of $f(T) = T^n - T$. It's easily seen that this discriminant equals the discriminant of $T^{n-1} - 1$. So by Lemma 2.6, N_0 is a unit if $p \not| (n-1)$. □

The next theorem is well-known. A good reference is [5].

Theorem 2.7. *Let $f(T) \subseteq R[T]$ be an irreducible monic polynomial of degree n and let S be the extension of R obtained by adjoining a root of f. If a height one prime qR ramifies under this extension, then q divides the discriminant of f.*

Proof. Let K and L denote the quotient fields of R and S, respectively. Let v be the (q)-adic valuation of R and let $v_1, \ldots, v_k$ denote the valuations of L which are extensions of v. Let n_i and e_i denote respectively the relative degree and reduced ramification index of v_i with respect to v. Then by Theorem 19 of [5, p. 55],

$$e_1 n_1 + \cdots + e_k n_k \leq n.$$

If qR ramifies, then $e_i > 1$ for some i. Thus, $n_1 + \cdots + n_k < n$.

Let R_i denote the valuation ring of v_i and let M_i be its maximal ideal. let σ be a root of f. Then σ satisfies a degree n_i polynomial modulo M_i. Hence σ satisfies a degree $n_1 + \cdots + n_k$ polynomial over $\cap_{i=1}^{k} M_i$. Since there are n such roots σ, we must have $\sigma_i - \sigma_j \in \cap_{i=1}^{k} M_i$ for two roots σ_i, σ_j of f. Hence, some power of $\sigma_i - \sigma_j$ is in qS, which implies that a power of Δ_f is in qR. Hence $\Delta_f \in qR$, as desired. □

Finally, we recall some useful information about valuations.

Theorem 2.8. *Let v be a valuation of a field K and let L be any field containing K. Then v can be extended to a valuation v^* of L.*

Proof. See Theorem 5′, p. 13 and p. 35 of [5]. □

Remark 2.1. If v is any valuation, then a simple consequence of the definition is that $v(\sum_{i=1}^{n} x_i) \geq \min\{v(x_1), \ldots, v(x_n)\}$, and equality holds if the minimum is attained by only one of the x_i.

Let R be a regular local ring and $I = (x, y)R$ a height two prime ideal. We may construct a valuation on the quotient field of R as follows. Let a and b be positive integers. Let $S = R_I[t]$, where $t^a = x$. This is a two dimensional regular local ring with maximal ideal $(t, y)S$. Now adjoin $u = y/t^b$ and consider $A = S[u]_{(t)}$. Since the maximal ideal of A is principal, A is a discrete valuation ring and there exists a valuation v on the quotient field of A defined by $v(\alpha t^n) = n$ if α is a unit of A. This restricts to a valuation on the quotient field of R. Notice that $v(x) = v(t^a) = a$ and, since u is a unit of A, $v(y) = v(ut^b) = b$. Further, we may express any element of R as a polynomial $f(x, y) = \sum_{(e,f)\in B} r_{(e,f)} x^e y^f$ where each $r_{(e,f)} \notin I$ and $B = \{(e_i, f_i) \mid 1 \leq i \leq k, e_1 < \cdots < e_k, f_1 > \cdots > f_k\}$. We claim that $v(f)$ is simply the infimum over the values of the monomials. It suffices to prove that monomials of the same value cannot sum to an element of higher value. Suppose that $v(z_1) = v(z_2) = \cdots = v(z_k)$ where $z_i = r_i x^{e_i} y^{f_i} = r_i u^{f_i} t^{ae_i + bf_i}$, $f_1 > \cdots > f_k$.

Then $ae_i + bf_i = ae_j + bf_j$ for all $1 \leq i, j \leq k$. If $v(z_1 + \cdots + z_k) > ae_i + bf_i$ then $r_1 u^{f_1 - f_k} + \cdots + r_{k-1} u^{f_{k-1} - f_k} + r_k = 0$ in the residue field of A. But the residue field of A is clearly $K(u)$ where K is the quotient field of R/I, so we must have $v(z_1 + \cdots + z_k) = ae_i + bf_i$.

Chapter 3

Sufficient Conditions

In this chapter we will present some conditions which ensure that an element $z \in R^+$ is actually in IR^+. The first theorem (Theorem 2.13 of [2]) in equicharacteristic p gives the plus closure form of the generalized Briançon-Skoda theorem of Hochster and Huneke [3, p. 45].

Theorem 3.1. *Let R be an integral domain and $I = (x_1, \ldots, x_n)$ an ideal of R. Suppose $p \in \sqrt{(x_1, x_2)R}$ and $z \in \overline{I^{n+k}}$ with $k \geq 0$. Then there exists an integral extension S of R with $z \in I^{k+1}S$.*

Lemma 3.2. *Let R be a local ring and p the characteristic of its residue field. Then given $0 \leq j \leq i \leq p^n$, and an integer m relatively prime to p, there is a unit u_{ij} such that*

$$\binom{p^n m - j}{i - j} = u_{ij} \binom{p^n - j}{i - j}.$$

In fact,

$$u_{ij} = \frac{(p^n m - j)!(p^n - i)!}{(p^n m - i)!(p^n - j)!}.$$

Proof. Fix i and p as above. Write u_j for u_{ij}. Clearly $u_i = 1$. Assume that for some $j+1 \leq i$ we have such a unit u_{j+1}. Then,

$$\begin{aligned}
\binom{p^n m - j}{i - j} &= \frac{(p^n m - j)!}{(i-j)!(p^n m - i)!} \\
&= \frac{(p^n m - j)(p^n m - (j+1))!}{(i-j)(i-(j+1))!(p^n m - i)!} \\
&= \frac{p^n m - j}{i - j}\binom{p^n m - (j+1)}{i - (j+1)} \\
&= u_{j+1}\frac{p^n m - j}{i - j}\binom{p^n - (j+1)}{i - (j+1)} \\
&= u_{j+1}\frac{p^n m - j}{i - j}\frac{(p^n - (j+1))!}{(i-(j+1))!(p^n - i)!} \\
&= u_{j+1}\frac{p^n m - j}{i - j}\frac{i - j}{p^n - j}\binom{p^n - j}{i - j} \\
&= u_{j+1}\frac{p^n m - j}{p^n - j}\binom{p^n - j}{i - j}
\end{aligned}$$

Thus $u_j = u_{j+1}\frac{p^n m - j}{p^n - j}$ is the desired unit. One can easily check that $u_{ij} = \frac{(p^n m - j)!(p^n - i)!}{(p^n m - i)!(p^n - j)!}$. □

Proposition 3.3, interesting in its own right, will be used in proving Lemma 3.4 below.

Proposition 3.3. *Let R be an integrally closed ring and let $x, y, z \in R$. Suppose that $z \in (x, y)R^+$ with $z = \alpha x + \beta y$ where α satisfies an irreducible monic polynomial of degree $p^n m$ over R with $(p, m) = 1$. Then $z = \alpha' x + \beta' y$, for some $\alpha', \beta' \in R^+$ where α' satisfies a polynomial of degree p^n over R.*

Proof. Let β satisfy the irreducible polynomial $f(T) = T^N + b_1 T^{N-1} + \cdots + b_N$ over R. Since $z - \beta y = \alpha x$, we must have $N = p^n m$. Since R is integrally closed, $f(T)$ is irreducible over the quotient field of R. Thus, for any root $\hat{\beta}$ of $f(T)$, there is an automorphism of R^+ taking β to $\hat{\beta}$. Hence $z - \hat{\beta} y \in xR^+$ for all roots $\hat{\beta}$ of $f(T)$. Let $g(T) = \sum_{i=0}^{N} c_i T^{N-i}$ where $c_i = (-1)^i \sum_{j=0}^{i} \binom{p^n m - j}{i-j} b_j y^j z^{i-j}$. Then by Lemma 2.2 the roots of $g(T)$ are $\{z - \hat{\beta} y \mid \hat{\beta} \text{ is a root of } f(T)\}$. This implies that

$$\sum_{j=0}^{i} \binom{p^n m - j}{i - j} b_j y^j z^{i-j} \in (x^i)$$

for each $0 \leq i \leq p^n m$. By (2.3) we need to show that there exist elements $\{c_j\}$ in R such that for $0 \leq i \leq p^n$,

$$\sum_{j=0}^{i} \binom{p^n - j}{i - j} c_j y^j z^{i-j} \in (x^i), \tag{3.1}$$

and such that $c_0 = 1$.

By Lemma 3.2, we may satisfy the ith equation by taking $c_j = u_{ij} b_j$, for $0 \leq j \leq i$. But $c_j = \frac{u_{ij}}{u_{i0}} b_j$ for $0 \leq j \leq i$ also solves the ith equation and

$$\frac{u_{ij}}{u_{i0}} b_j = \frac{(p^n m - j)!(p^n)!}{(p^n m)!(p^n - j)!} b_j$$

does not depend on i, giving us a set $\{c_0, c_1, \ldots, c_{p^n}\}$ which solves all of the equations in (3.1) with $c_0 = 1$, as desired. □

Lemma 3.4. *Let R be integrally closed and let x, y, z be nonunit elements of R. Let $q_1 R, q_2 R, \ldots, q_k R$ be height one primes of R such that $x, y \notin q_i R$ for all i. Let w be an element of R^+ with $w = \alpha x + \beta y$ for some α, β integral over*

R. Then there exist α', β' integral over R such that $w = \alpha' x + \beta' y$, and none of $q_1 R, \ldots, q_k R$ ramify under the extension to $R[\alpha']$. If in addition $\alpha \in x^d \overline{R[\alpha]}$ for $d \leq 1$, then we can ensure that $\alpha' \in x^d \overline{R[\alpha']}$.

Proof. Let $f(T) = T^n + a_1 T^{n-1} + \cdots + a_n$ be the monic irreducible polynomial over R which has α as a root. We may assume that p does not divide $n-1$, for otherwise p and n are relatively prime and by Lemma 3.3 we may take $\alpha' \in R$. If β satisfies $T^n + b_1 T^{n-1} + \cdots + b_n$ over R, then $b_i y^i = (-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a_j x^j w^{i-j}$.

Let $a'_i = a_i$ for $i \neq n-1$ and $a'_{n-1} = a_{n-1} + l x^{n-1} y^n$, where $l \in R$ will be chosen later in the proof. Let $b'_i = b_i$ for $i < n-1$, $b'_{n-1} = b_{n-1} + (-1)^{n-1} l x^{2(n-1)} y$, and $b'_n = b_n + (-1)^n l x^{2(n-1)} w$. Then for $i < n-1$ certainly $(-1)^i \sum_{j=0}^{i} \binom{n-j}{i-j} a'_j x^j w^{i-j} = b'_i y^i$. When $i = n-1$,

$$\begin{aligned}
&(-1)^{n-1} \sum_{j=0}^{n-1} \binom{n-j}{n-1-j} a'_j x^j w^{n-1-j} \\
&= (-1)^{n-1} \left\{ \sum_{j=0}^{n-1} \binom{n-j}{n-1-j} a_j x^j w^{n-1-j} + l x^{2(n-1)} y^n \right\} \\
&= b_{n-1} y^{n-1} + (-1)^{n-1} l x^{2(n-1)} y^n \\
&= b'_i y^{n-1}.
\end{aligned}$$

Similarly, when $i = n$,

$$\begin{aligned}
(-1)^n \sum_{j=0}^{n} \binom{n-j}{n-j} a'_j x^j w^{n-j} &= (-1)^n \left\{ \sum_{j=0}^{n} \binom{n-j}{n-j} a_j x^j w^{n-j} + l x^{2(n-1)} y^n w \right\} \\
&= b_n y^n + (-1)^n l x^{2(n-1)} y^n w \\
&= b'_i y^n.
\end{aligned}$$

Let α' be a root of $\sum_{i=0}^{n} a_i' T^{n-i}$. Then by (2.3), $\beta' = (w - \alpha' x)/y$ is a root of $\sum_{i=0}^{n} b_i' T^{n-i}$. Hence $w = \alpha' x + \beta' y$. Also, since $\alpha \in x^d \overline{R[\alpha]}$, it follows that $a_i \in x^{di} R$ for all i. Then for $d \leq 1$, $a_i' \in x^{di} R$ for all i as well. Hence $\alpha' \in x^d \overline{R[\alpha']}$.

Finally, we show that we may choose l such that $q_1 R, \ldots, q_k R$ do not ramify. By (2.7), it suffices to prove that there exists an l such that for each i, q_i does not divide the discriminant of $\sum_{j=0}^{n} a_j' T^{n-j}$. Denote this discriminant by $\Delta(l)$. Since we are assuming that p does not divide $n-1$, by Proposition 2.5 for some unit integer N,

$$\begin{aligned} \Delta(l) &= N(a_{n-1} + l x^{n-1} y^n)^n + \text{lower degree terms in } a_{n-1} + l x^{n-1} y^n \\ &= (N x^{n(n-1)} y^{n^2}) l^n + \text{lower degree terms in } l. \end{aligned}$$

Modulo q_i, the coefficient $N x^{n(n-1)} y^{n^2} \not\equiv 0$ and so considering l to be an indeterminate, $\Delta(l) \not\equiv 0$. Modulo q_i there are at most n congruence classes which give roots of $\Delta(l)$.

Let $\mathcal{A} = \{y^j \mid j \geq 1\}$. This is an infinite set, all of whose members are distinct modulo q_1. So there exists some $y^t \in \mathcal{A}$ such that $\Delta(y^t) \not\equiv 0$ modulo q_1. Now we consider q_i for $i \geq 2$. The set $\mathcal{B} = \{y^t + q_1^m \mid m \geq 1\}$ is an infinite set, all of whose members are distinct modulo q_i. Thus, for each $i \geq 2$, there exists an integer m_i such that if $m \geq m_i$ then $\Delta(y^t + q_1^m) \not\equiv 0$ modulo q_i. Let $M = \max\{m_2, \ldots, m_k\}$ and let $l = y^t + q_1^M$. Then certainly $\Delta(l) \not\equiv 0$ modulo q_i for $i \geq 2$, and since $l \equiv y^t$ modulo q_1, $\Delta(l) \not\equiv 0$ modulo q_1. □

The information about the coefficients of the polynomial in the next proposition will be useful in Chapter 4.

Proposition 3.5. *Let x, y be nonunit elements of an integrally closed ring R, let p be an odd prime number and let $n = p^2$. Suppose that $p \in (y^c, x^{de})R$ where c, d, e, f are rational numbers such that $1/c + 1/d \leq f/3$ and $1/3 \leq e \leq 1$. Also suppose $z \in R^+$ satisfies $z^3 \in (y^c, x^d)^f R$. Further assume there exists $F \in R$ such that $z^{n-1} - Fx^{n-1}y^{n-1} \in (y^n, x^n)R$. Then there exist elements v, w integral over R such that $z = yv + xw$ where w can be chosen to be any root of $T^n + a_1T^{n-1} + \cdots + a_n = 0$, with each a_i in an integral extension S of $R[z]$. We may choose our coefficients so that, modulo the integral closure of some fractional power of x in S, $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Fy^{n-1}$, and $a_n \equiv r$ for some element $r \in R$. Furthermore, we can ensure that for any finite set of height one primes $q_1R, \ldots, q_kR$ such that $x, y \notin q_iR$ for all i, there is no ramification under the extension to $R[a_1, \ldots, a_n]$.*

Proof. Suppose that $c = c_1/c_2$ and $d = d_1/d_2$ where c_1, c_2, d_1, d_2 are integers. Let $R' = R[z, s, u]$, where $s^{3c_2} = y$ and $u^{3d_2} = x$. We shall construct the polynomial $T^n + a_1T^{n-1} + \cdots + a_n$ and let w be a root. By Lemma 2.3 with $a_0 = 1$, we will have v integral over R if for some integral extension S of R' we satisfy $\sum_{j=0}^{i} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j} = b_i s^{3c_2 i}$ with $b_i \in S$ for $i = 1, \ldots, n$. We inductively define $a_1, \ldots, a_{n-1}$ to satisfy the first $n-1$ equations and also to satisfy $a_j u^{3d_2 j} \in (s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fj-1}\overline{(s^{c_1}, u^{d_1})S_j}$ where S_j is an integral extension of R' and $S_j \subseteq S_i$ for $j < i$. We then let $S = S_n$. To satisfy the i^{th} equation, we must define a_i, b_i so that $\sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j} = b_i s^{3c_2 i} - a_i u^{3d_2 i}$. Of course, $a_0 = 1$.

First consider $i < n$. Since $z^3 \in (s^{c_1}, u^{d_1})^{3f} R'$, it follows that $z^i \in \overline{(s^{c_1}, u^{d_1})^{fi} R'}$. Hence, when $j \neq 0$ we have $a_j u^{3d_2 j} z^{i-j} \in (s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fj-1}$ $\overline{(s^{c_1}, u^{d_1})^{f(i-j)+1} S_j}$. Applying (3.1) we see that this last ideal is contained in $(s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1}) S_{j_0}}$, for some integral extension S_{j_0} of S_j. When $j = 0$ and $i < n$, the term $\binom{n}{i} z^i \in p\overline{(s^{c_1}, u^{d_1})^{fi} R'} \subseteq (s^{3c_1}, u^{3d_1 e})$ $(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1}) S_{i_1}}$, where S_{i_1} is an integral extension of R'. Let S_i be an integral extension of R' containing S_{i_0} and S_{j_0} for $1 \leq j < i$. Then the left hand side of the equation is in $(s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1}) S_i}$. Any generator of $(s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1} S_i$ which is not a multiple of $s^{3c_2 i}$ must be a multiple of u^l, where $l \geq d_1(fi - 1 - 3(\frac{c_2}{c_1})i + \frac{1}{c_1}) + 3d_1 e$. Since $\frac{c_2}{c_1} \leq \frac{f}{3} - \frac{d_2}{d_1}$, we obtain $l \geq 3d_2 i - d_1 + \frac{d_1}{c_1} + 3d_1 e > 3d_2 i$, since $3e \geq 1$. So we may solve the equation with $a_i u^{3c_2 i} \in (s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fi-1}\overline{(s^{c_1}, u^{d_1}) S_i}$. Notice that since $l > 3d_2 i$, we may choose $a_i \in uS_i$, which implies that $a_i \in u\overline{R'[a_i]}$.

Suppose that we have chosen $a_1, \ldots, a_{i-1}$ such that $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[a_1, \ldots, a_{i-1}]$. Let $w_i = \sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j u^{3d_2 j} z^{i-j}$. Then $w_i = b_i s^{3c_2 i} - a_i u^{3d_2 i}$. By (3.4) we may replace our original choice of a_i, b_i with elements a_i', b_i', integral over R with the additional property that $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[a_i']$. Note that (3.4) allows us to maintain our assumption that $a_i \in u\overline{R'[a_i]}$.

Finally, the $i = n$ case differs only in the $j = 0$ term. Thus the left hand side of the equation equals $z^n + G$ where $G \in (s^{3c_1}, u^{3d_1 e})(s^{c_1}, u^{d_1})^{fn-1}$ $\overline{(s^{c_1}, u^{d_1}) S_n} \subseteq (u^{3d_2 n}, s^{3c_2 n}) S_n$. Say $G = u^{3d_2 n}\alpha + s^{3c_2 n}\beta$, where we have chosen α as above so that $\alpha \in \overline{uR'[\alpha]}$ and $q_1 R, \ldots, q_k R$ do not ramify under the extension to $R'[\alpha]$. Now, $z^n - F s^{3c_2(n-1)} u^{3d_2(n-1)} z = u^{3d_2 n} r_1 + s^{3c_2 n} r_2$ for some

elements $r_1, r_2 \in R$. Replacing a_{n-1} with $a_{n-1} - Fu^{3d_2(n-1)}$ still allows us to solve the $(n-1)^{\text{st}}$ equation (with a different b_{n-1}) and also enables us to solve the n^{th} equation since the left hand side of that equation is now

$$z^n + G - Fs^{3c_2(n-1)}u^{3d_2(n-1)}z = u^{3d_2 n}(r_1 + \alpha) + s^{3c_2 n}(r_2 + \beta).$$

In fact, we may choose $a_n = r_1 + \alpha$, satisfying the desired condition. □

Corollary 3.6. *With the notation and assumptions of Proposition 3.5, there exist elements v, w integral over R such that $z = yv + xw$ where w can be chosen to be any root of $T^n + a_1T^{n-1} + \cdots + a_n = 0$ and we may choose our coefficients so that each a_i is in an integral extension S of R such that given a height one prime qR with $x, y \notin qR$ and $z^3 \in qR$, then qR does not ramify under the extension to $S[w]$, and modulo the integral closure of some fractional power of x, $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Fy^{n-1}$, and $a_n \equiv r$ for some $r \in R$.*

Proof. Let $q_1, \ldots, q_k$ be the height one primes with the property that $z^3 \in q_iR$, and $x, y \notin q_iR$. First we apply (3.5) to find an element $w \in R^+$ such that $z = xv + yw$ and w satisfies $T^n + a_1T^{n-1} + \cdots + a_n$ over S (an integral extension of R[z]) where the desired conditions on the a_i are satisfied. Applying (3.4) (with y in place of x) we may assume that $q_1R, \ldots, q_kR$ do not ramify under the extension to $S[w]$. Recall that in the proof of (3.4) no changes are made to $a_1, \ldots, a_{n-2}$ and a_n, while a_{n-1} is replaced by $a_{n-1} + ly^{n-1}x^n$. So the coefficients of the new polynomial will also satisfy the desired conditions. □

Theorem 3.11 below and its corollaries are our strongest sufficient conditions. First we need a few lemmas.

Lemma 3.7. *Suppose i, j are positive integers and $n = i + j$. Let $a_k \dots a_0$ be the expression for i in base p, i.e., $i = a_0 + a_1 p + \cdots + a_k p^k$ with $0 \leq a_j < p$. Similarly, suppose $j = b_k \dots b_0$, $n = c_k \dots c_0$. Let $d = |\{j \mid a_j + b_j > c_j\}|$. Then d is the highest power of p which divides $\binom{n}{i}$.*

Proof. This is Lemma 2.5 of [1]. The statement here is slightly stronger, but this is what is actually proven in [1]. □

The next lemma is taken from [1, Theorem 2.8]

Lemma 3.8. *Let $\mu, p \in R$ with $\mu^p = p$. For $1 \leq i < p^L$, let $\phi(i)$ denote the sum of the digits when $p^L - i$ is written in base p. Then*

$$(a) \quad \mu^{\phi(i)+1} \mid \binom{p^k}{i + p^k - p^L}, \quad \text{for } k \leq L,$$

$$(b) \quad \mu^{\phi(i)+1} \mid \binom{p^L}{i}, \text{ and}$$

$$(c) \quad \mu^{\phi(i)-\phi(j)+1} \mid \binom{p^L - j}{i - j}.$$

Proof. We begin by proving (a) and note that the $k = L$ case gives (b). Let d denote the number of nonzero digits when $p^L - i$ is written in base p. Then $\phi(i) \leq (p-1)d < pd$. Since $\binom{p^k}{i+p^k-p^L} = \binom{p^k}{p^L-i}$, Lemma 3.7 shows that $p^d \mid \binom{p^k}{i+p^k-p^L}$.

For (c), note that $\binom{p^L-j}{i-j} = \binom{p^L-j}{p^L-i}$. Expressing $p^L - i$ and $p^L - j$ in base p, let d denote the number of digits of $p^L - i$ which are larger than the corresponding digits of $p^L - j$. Then, since at least one digit of $p^L - j$ must be larger, $\phi(i) - \phi(j) \leq d(p-1) - 1$. Lemma 3.7 gives $p^d \mid \binom{p^L-j}{p^L-i}$, completing the proof. □

Lemma 3.9. *Let $I = (s, u)$ be an ideal of R and e_1, e_2, f, q, k be positive integers such that $q \geq e_1 + e_2 + kf$ and $e_1 \geq f$. Further assume $s^j \in (u^{\lfloor fj/e_1 \rfloor})$ for every j. Then $I^{qj} \subseteq (s^{e_1 j}, u^{(e_2+(k+1)f)j})$.*

Proof. Observe that I^{qj} is generated by monomials $s^A u^{qj-A}$. If $A \leq e_1 j - 1$, then since $s^A \in (u^{\lfloor Af/e_1 \rfloor})$, the power of u obtained is

$$\begin{aligned}
\lfloor \frac{Af}{e_1} \rfloor + qj - A &> \frac{Af}{e_1} + qj - A - 1 \\
&\geq (e_1 + e_2 + kf)j - A(1 - \frac{f}{e_1}) - 1 \\
&\geq (e_1 + e_2 + kf)j - (e_1 j - 1)(1 - \frac{f}{e_1}) - 1 \\
&= (e_2 + (k+1)f)j + (1 - \frac{f}{e_1}) - 1 \\
&\geq (e_2 + (k+1)f)j - 1,
\end{aligned}$$

Hence $\lfloor \frac{Af}{e_1} \rfloor + qj - A \geq (e_2 + (k+1)f)j$ as desired. □

Lemma 3.10. *Let R be a ring and $I = (s,u)R$. Let $h \geq 2, q, e_1, e_2, f, k$ be positive integers with $q \geq e_1 + e_2 + kf$ and $e_1 \geq f+2$ such that $s^j \in (u^{\lfloor fj/e_1 \rfloor})$. Then*

$$I^{hq(q-1)} \subseteq [s^{e_1 hq}, u^{(e_2+(k+1)f)hq}, (s^{e_1}u^{e_2+kf})I^{hq(q-1)-q}].$$

Proof. Again, $I^{hq(q-1)}$ is generated by monomials $s^A u^{hq(q-1)-A}$ and we may assume that $A \leq e_1 hq - 1$. Then $hq(q-1) - A \geq hq(q-e_1-1)+1 \geq h(e_1+e_2+kf)(e_2+kf-1)+1 \geq e_2+kf$, so we only need to consider the case where $A \leq e_1 - 1$. Then the power of u obtained is

$$\begin{aligned} \lfloor \frac{Af}{e_1} \rfloor + hq(q-1) - A &> hq(q-1) + \frac{Af}{e_1} - A - 1 \\ &= hq(q-1) - A(1 - \frac{f}{e_1}) - 1 \\ &\geq hq(q-1) - (e_1 - 1)(1 - \frac{f}{e_1}) - 1 \\ &= hq(q-1) - (e_1 - f - 1) - \frac{f}{e_1} - 1 \end{aligned}$$

Now, since $e_1 \geq f+2$, certainly $(hq-1)e_1(e_1-f-1) \geq f$. Hence $hq(e_1-f-1) - (e_1-f-1) \geq \frac{f}{e_1}$, and so $hq(e_1+e_2+kf-1) - (e_1-f-1) - \frac{f}{e_1} \geq hq(e_2+(k+1)f)$. We have now shown that $\lfloor \frac{Af}{e_1} \rfloor + hq(q-1) - A > hq(e_2+(k+1)f) - 1$ and so $s^A u^{hq(q-1)-A} \in (u^{(e_2+(k+1)f)hq})$. □

Theorem 3.11. *Let R be a $\mathbb{Z}$-graded integral domain. Let $\mu \in R$ such that $\mu^p = p$. Let s, u, z be homogeneous elements of R with $\deg(s) = \deg(z) = 0$, $\deg(u) = -1$. Let $I = (s,u)R$. Suppose q, e_1, e_2, f, k are positive integers with*

$q \geq e_1 + e_2 + kf$ and $e_1 \geq f + 2$. Further assume $z \in \overline{I^q}$, $\mu z^j \in I^{qj}$, and $s^j \in (u^{\lfloor fj/e_1 \rfloor})$ for every j. Then there exists a g-integral extension S of R and elements $\alpha, \beta \in S$ such that $z = s^{e_1}\alpha + u^{e_2+(k+1)f}\beta$, where α is homogeneous of degree zero.

Proof. First we reduce to the Noetherian case. If R is not Noetherian, we may replace R by a Noetherian subdomain in which the entire hypothesis is satisfied. To see this, note that $z \in \overline{I^q}$ means that there exists a positive integer h such that $z^{h+1} \in I^q(I^q, z)^h$. Thus this condition is simply the existence of a finite set of elements satisfying a particular equation. Next note the condition $\mu z^j \in I^{qj}$ for every j now reduces to the condition $\mu z^j \in I^{qj}$ for every $j \leq h$ and so simply requires the existence of a finite set of elements satisfying a finite set of equations. Finally, the condition that $s^j \in (u^{\lfloor fj/e_1 \rfloor})$ for every j is equivalent to the condition that $s^j \in (u^{\lfloor fj/e_1 \rfloor})$ for every $j \leq e_1$. Thus we may replace R by a finitely generated $\mathbb{Z}$-algebra containing the prescribed set of elements.

Next we derive an equation for z^n, for some large n, which will be used in the final step of the proof. To this end, define a family of modules

$$C_i = (I^q, z)^i / (s^{e_1 i}, u^{(e_2+(k+1)f)i})$$

and homomorphisms $g_{ij} : C_i \longrightarrow C_j$ with $i < j$ by $g_{ij}(\overline{c}) = \overline{(s^{e_1}u^{e_2+kf})^{j-i}c}$. This map is well-defined since $s^{e_1} \in (u^f)R$. We claim that for every $N \geq hq$, $I^{q(N-h)} \subseteq (s^{e_1 N}, u^{(e_2+(k+1)f)N}, (s^{e_1}u^{e_2+kf})I^{q(N-h)-q})$. This is true for $N = hq$ by Lemma 3.10. Assume that this holds for some $N \geq hq$ and consider

$I^{q(N+1-h)} = I^{q(N-h)}I^q$. Since Lemma 3.9 gives $I^q \subseteq (s^{e_1}, u^{e_2+(k+1)f})$, it follows that

$$I^{q(N+1-h)} \subseteq (s^{e_1(N+1)}, u^{(e_2+(k+1)f)(N+1)}, (s^{e_1}u^{e_2+kf})I^{q(N+1-h)-q}),$$

which proves the claim. Using the integer h mentioned above, the condition $z^{h+1} \in I^q(I^q, z)^h$ implies that $(I^q, z)^N = I^{q(N-h)}(I^q, z)^h$ for all $N > h$. This implies that every nonzero monomial in C_N, $N \geq hq$, will be divisible by $s^{e_1}u^{e_2+kf}$ and so $C_N = g_{N-1,N}(C_{N-1})$. Hence $g_{N-1,N}$ is onto for every $N \geq hq$. Thus $C = \varinjlim C_i$ is a homomorphic image of C_{hq-1} and so it is a Noetherian module. We then see that $\cup \ker(g_{hq-1,j})$ is finitely generated and it follows that $C = C_M$ for sufficiently large M.

Next, for each positive integer k, regard z^{p^k} as an element of C by first regarding it as an element of C_{p^k}. Let $B = \{\overline{z^{p^k}} \mid k \geq 1\}R$. Since B is a submodule of C, it is finitely generated and so there exists an integer K with $B = \{\overline{z^{p^k}} \mid 1 \leq k \leq K\}R$. Choose L sufficiently large so that $p^L > M, p^K$. Then, as $\overline{z^{p^L}} \in B$, we obtain an equation

$$z^{p^L} = \sum_{k=1}^{K} r_k(s^{e_1}u^{e_2+kf})^{p^L-p^k}z^{p^k} + s^{e_1p^L}v + u^{(e_2+(k+1)f)p^L}w \tag{3.2}$$

with $\deg(r_k) = (e_2+kf)(p^L-p^k)$, $\deg(v) = 0$, and $\deg(w) = (e_2+(k+1)f)p^L$. This is the desired equation. We shall employ it later in the proof. We have no further use of the modules B and C.

Let $n = p^L$. By Lemma 2.3, to obtain $z - s^{e_1}\alpha = u^{e_2+(k+1)f}\beta$ it suffices to find elements $a_1, \ldots, a_n$ and $b_1, \ldots, b_n$ such that for $1 \leq i \leq n$,

$$\sum_{j=0}^{i} \binom{n-j}{i-j} a_j s^{e_1 j} z^{i-j} = u^{(e_2+(k+1)f)i} b_i,$$

where $\deg(a_j) = 0$.

We will define the elements $a_1, \ldots, a_n$ indirectly by choosing elements $c_1, \ldots, c_n$ such that

$$a_i = \begin{cases} c_i - r_k u^{(e_2+kf)(p^L-p^k)}, & \text{for } i = p^L - p^k, \ \ 1 \le k \le K \\ c_i - v, & \text{for } i = n \\ c_i, & \text{otherwise.} \end{cases}$$

We will require that $c_i \in \mu^{\phi(i)} I^{(e_2+kf)i}$ for each i, where $\phi(i)$ denotes the sum of the digits when $p^L - i$ is written in base p. To obtain $\deg(a_i) = 0$ it suffices to ensure that $\deg(c_i) = 0$ for all i. Simultaneously, recalling that $s^{e_1} \in (u^f)R$, we will choose $d_1, \ldots, d_n$ and set

$$b_i = \begin{cases} d_i - r_k(\frac{s^{e_1}}{u^f})^{p^L-p^k}, & \text{for } i = p^L - p^k, \ \ 1 \le k \le K \\ d_i + w, & \text{for } i = n \\ d_i, & \text{otherwise.} \end{cases}$$

We choose c_1 as follows. The first equation is $\binom{p^L}{1} z + \binom{p^L-1}{0} a_1 s^{e_1} = u^{e_2+(k+1)f} b_1$. As $c_1 = a_1$ and $d_1 = b_1$, this can be written as $p^L z + c_1 s^{e_1} = u^{e_2+(k+1)f} d_1$, or alternatively, since $\mu^p = p$, as $\mu^{pL} z + c_1 s^{e_1} = u^{e_2+(k+1)f} d_1$. Now by Lemma 3.9, $\mu z \in I^q \subseteq (s^{e_1}, u^{e_2+(k+1)f})$ and has degree 0. So we may solve this equation with $c_1 \in \mu^{pL-1} I^{e_2+kf}$ and $\deg(c_1) = 0$. Now, $\phi(1) = (p-1)L$ as $p^L - 1$ has L digits, each equalling $(p-1)$. As $(p-1)L \le pL - 1$, we have in fact chosen $c_1 \in \mu^{\phi(1)} I^{e_2+kf}$.

Now suppose we have chosen $c_j \in \mu^{\phi(j)} I^{(e_2+kf)j}$ with $\deg(c_j) = 0$ for each $j < i$ so that the first $i-1$ equations are satisfied. We want to choose c_i, d_i to satisfy

$$\sum_{j=0}^{i-1} \binom{n-j}{i-j} a_j s^{e_1 j} z^{i-j} + a_i s^{e_1 i} = u^{(e_2+(k+1)f)i} b_i.$$

First suppose $i < p^L$. Note that $u^{(e_2+(k+1)f)i}b_i - s^{e_1 i}a_i = u^{(e_2+(k+1)f)i}d_i - s^{e_1 i}c_i$ for all i. Let E be the smallest integer such that $p^L - p^E < i$. Then we must satisfy

$$\binom{p^L}{i}z^i + \sum_{j=1}^{i-1}\binom{n-j}{i-j}c_j s^{e_1 j}z^{i-j} - \sum_{k=E}^{K}\binom{p^k}{i+p^k-p^L}r_k\big(s^{e_1}u^{e_2+kf}\big)^{(p^L-p^k)}z^{i+p^k-p^L} = u^{(e_2+(k+1)f)i}d_i - s^{e_1 i}c_i.$$

[The final sum is vacuous if $E > K$.] To find the desired $c_i \in \mu^{\phi(i)}I^{(e_2+kf)i}$, it is sufficient to show each term is in $\mu^{\phi(i)}I^{qi}$ by Lemma 3.9. Since each term in the left hand side of the equation has degree zero, we may then choose c_i to be homogeneous of degree zero.

By Lemma 3.8, $\mu^{\phi(i)+1} \mid \binom{p^L}{i}$. As $\mu z^i \in I^{qi}$, this yields $\binom{p^L}{i}z^i \in \mu^{\phi(i)}I^{qi}$. Similarly, Lemma 3.8 gives $\binom{n-j}{i-j}c_j s^{e_1 j}z^{i-j} \in \mu^{\phi(i)-\phi(j)+1}\mu^{\phi(j)}I^{qj}z^{i-j} \subseteq \mu^{\phi(i)}(\mu z^{i-j})I^{qj} \subseteq \mu^{\phi(i)}I^{qi}$. Finally, $\binom{p^k}{i+p^k-p^L}r_k\big(s^{e_1}u^{e_2+kf}\big)^{(p^L-p^k)}z^{i+p^k-p^L} \in \mu^{\phi(i)+1}I^{q(p^L-p^k)}z^{i+p^k-p^L} \subseteq \mu^{\phi(i)}I^{qi}$. Therefore we may find the appropriate c_i for $i < n = p^L$.

Lastly, we must deal with the case $i = p^L$. Since $\binom{n-j}{n-j} = 1$, the equation we must solve is

$$\sum_{j=0}^{n-1}a_j s^{e_1 j}z^{n-j} + a_n s^{e_1 n} = u^{(e_2+(k+1)f)n}b_n.$$

Again, substituting c_j's and d_j's, this is equivalent to

$$z^n + \sum_{j=1}^{n-1}c_j s^{e_1 j}z^{n-j} - \sum_{k=1}^{K}r_k\big(s^{e_1}u^{e_2+kf}\big)^{p^L-p^k}z^{p^k} + c_n s^{e_1 n} - v s^{e_1 n} = u^{(e_2+(k+1)f)n}d_n + u^{(e_2+(k+1)f)n}w.$$

Combining this equation with our derived equation (3.2), we get the simplified equation

$$\sum_{j=1}^{n-1} c_j s^{e_1 j} z^{n-j} = u^{(e_2+(k+1)f)n} d_n - c_n s^{e_1 n}.$$

Now $c_j s^{e_1 j} \in \mu^{\phi(j)} I^{qj} \subseteq \mu I^{qj}$ for all j and since $\mu z^{n-j} \in I^{q(n-j)}$, each term in the left hand sum is contained in I^{qn}. As usual, this allows us to find the desired c_n, d_n to complete the proof. [Again, since each term of the summation has degree 0, we can ensure that $\deg(c_n) = 0$.] □

Corollary 3.12. *Let R be an integrally closed integral domain and $I = (x_1, x_2)$ an ideal with $p \in \sqrt{I}$. Let a, b, c, d be positive integers with $c > b$ and $\frac{1}{b} + \frac{1}{c} \leq \frac{d}{a}$. Suppose $z^a \in (t^b, I^c)^d$ where $t \in I$. Then $z \in IR^+$.*

Proof. Replace R by $R[\mu]$ where $\mu^p = p$. Since $p \in \sqrt{I}$, there exists an integer m such that $\mu^m \in I^2$. Let $e = cm$, $f = bm$, and $q = e + f$. Let $A = R[\mu, s, v_1, v_2]$ with $s^e = t$, and $v_i^f = x_i$. Let $J = (v_1, v_2)A$. Then $z^a \in (s, J)^{bcdm} A$ and so $z^j \in \overline{(s, J)^{(b+c)mj}} A = \overline{(s, J)^{qj}} A$ for every j. Now $\mu^m \in I^2 \subseteq J^{2f} \subseteq J^{2m}$ and so $\mu \in \overline{J^2}$. Thus for every j, $\mu z^j \in \overline{(s, J)^{qj+2}}$. By Theorem 3.1, this implies that for every j, $\mu z^j \in (s, J)^{qj} A'$ for some integral extension A' of A. Also, note that $s^e \in J^f$, and so $s^j \in \overline{J^{\lfloor fj/e \rfloor}}$ for all j.

Let S be the integral closure of the extended Rees ring, $A'[Jt, u]$, where $u = t^{-1}$. This is a graded ring in which the intersection of the ideal (u^n) with the degree zero summand is equal to the integral closure of J^n in A'. Note that

we now have $s^j \in (u^{\lfloor fj/e \rfloor})S$, $z^j \in \overline{(s,u)^{qj}}$, and $\mu z^j \in (s,u)^{qj}$ and $s^j, z^j, \mu z^j$ all have degree zero. We may now apply Theorem 3.11 with $e_1 = e$, $e_2 = 0$, and $k = 1$, if necessary replacing m by a larger integer to ensure $e \geq f + 2$. Thus, $z - s^e\alpha = u^{2f}\beta$ where α, β are elements of some g-integral extension of S and $\deg(\alpha) = 0$. Since the intersection of the degree zero summand of S with $(u^{2f})S$ is equal to $\overline{(v_1, v_2)^{2f}A'} = \overline{(x_1, x_2)^2 A'} \subseteq IR^+$, this completes the proof. □

Corollary 3.13. *Let R be an integrally closed integral domain and $I = (x_1, \ldots, x_{k+1})$ an ideal with $p \in \sqrt{I}$. Suppose $a, b_1, \ldots, b_k, c, d$ are positive integers such that $c > b_1$, and $t_1, \ldots, t_k \in I$ with $z^a \in (t_1^{b_1}, \ldots, t_k^{b_k}, I^c)^d$ where $\frac{1}{b_1} + \cdots + \frac{1}{b_k} + \frac{k}{c} \leq \frac{d}{a}$. Then $z \in IR^+$.*

Proof. Replace R by $R[\mu]$ where $\mu^p = p$. Since $p \in \sqrt{I}$, there exists an integer m such that $\mu^m \in I^{2k}$. Let $e_i = b_1 \cdots b_k cm/b_i$, $f = b_1 \cdots b_k m$, and $q = e_1 + \cdots + e_k + kf$. Let $A = R[\mu, s_1, \ldots, s_k, v_1, \ldots, v_{k+1}]$ with $s_i^{e_i} = t_i$, and $v_i^f = x_i$. Let $J = (v_1, \ldots, v_{k+1})A$. Then $z^a \in (s_1, \ldots, s_k, J)^{b_1 \cdots b_k cdm} A$ and so $z^j \in \overline{(s_1, \ldots, s_k, J)^{(e_1 + \cdots + e_k + kf)j} A} \subseteq \overline{(s_1, \ldots, s_k, J)^{qj} A}$ for every j. Now $\mu^m \in I^{2k} \subseteq J^{2kf} \subseteq J^{2km}$ and so $\mu \in \overline{J^{2k}}$. Thus for every j, $\mu z^j \in \overline{(s_1, \ldots, s_k, J)^{qj+2k}} A$. By Theorem 3.1, this implies that for every j, $\mu z^j \in (s_1, \ldots, s_k, J)^{qj} A'$ for some integral extension A' of A. Also, note that $s_i^{e_i} \in J^f$, and so $s_i^j \in \overline{J^{\lfloor fj/e_i \rfloor}}$ for all j.

Let $\tilde{J}$ be the ideal $(s_2, \ldots, s_k, J)A'$ and let S be the integral closure of the extended Rees ring, $A'[\tilde{J}t, u]$, where $u = t^{-1}$. This is a graded ring in

which the intersection of the ideal (u^n) with the degree zero summand is equal to the integral closure of $\tilde{J}^n$ in A'.

Note that we now have $s_1^j \in (u^{\lfloor fj/e_1 \rfloor})S$, $z^j \in \overline{(s_1, u)^{qj}}$, $\mu z^j \in (s_1, u)^{qj}$, and $s_1^j, z^j, \mu z^j$ all have degree zero. We may now apply Theorem 3.11, if necessary replacing m by a larger integer to ensure $e_1 \geq f+2$, and with $e_2+\cdots+e_k$ in place of e_2. This gives $z - s_1^{e_1}\alpha = u^{e_2+\cdots+e_k+(k+1)f}\beta$ for some α, β in a g-integral extension of R with $\deg(\alpha) = 0$. The intersection of the degree zero summand of S with $(u^{e_2+\cdots+e_k+(k+1)f})S$ is equal to $\overline{(s_2, \ldots, s_k, J)^{e_2+\cdots+e_k+(k+1)f}}A' \subseteq (s_2, \ldots, s_k, J)^{e_2+\cdots+e_k+(k+1)f-2k+1}R^+$, by Theorem 3.1. This last ideal is contained in $(s_2^{e_2}, \ldots, s_k^{e_k}, J^{(k+1)f-k})R^+$. Now,

$$J^{(k+1)f-k} = (v_1, \ldots, v_{k+1})^{(k+1)f-k} \subseteq (v_1^f, \ldots, v_{k+1}^f) = I.$$

It follows that $(s_2^{e_2}, \ldots, s_k^{e_k}, J^{(k+1)f-k})R^+ \subseteq IR^+$, thereby completing the proof. □

We can now prove the reverse implication of Conjecture 1.2. Conditions (3), (4), and (5) below represent the best information that Corollary 3.12 gives when $z^3 \in R$.

Corollary 3.14. *Let R be a regular local ring and let x, y be part of a regular system of parameters for R. Suppose p is a prime number and $p \in I = (x, y)R$.*

Let $z^3 \in R$ and suppose that one of the following holds:

(1) $z^3 \in t^3R$ *for some* $t \in I$

(2) $z^3 \in I^6$

(3) $z^3 \in (t, I^3)^4$ *for some* $t \in I$

(4) $z^3 \in (t, I^2)^5$ *for some* $t \in I$

(5) $z^3 \in (t^5, I^8)$ *for some* $t \in I$.

Then $z \in IR^+$.

Proof. If $z^3 \in t^3R$, then z/t is integral over R. Hence $z \in tR^+$. If $z^3 \in I^6$, then $z \in \overline{I^2}$ and then Theorem 3.1 implies that $z \in IR^+$. The remaining cases follow directly from Corollary 3.12. □

Chapter 4

Necessary Conditions

The following well known lemma can be found in [2].

Lemma 4.1. *Let R be a regular local ring with x, y part of a regular system of parameters. Let w be a root of a monic irreducible polynomial $f(T) \in R[T]$ and suppose $w \in \overline{(x,y)S}$ for some integral extension S of R. If $f(T) = T^n + a_{n-1}T^{n-1} + \cdots + a_n$, then $a_i \in (x,y)^i R$ for every i.*

The next lemma is Lemma 3.2 of [2] and is a powerful tool for proving that elements are not in the plus closure.

Lemma 4.2. *Let R be an integrally closed Henselian domain with residue field K. Suppose $z \in R^+$ is in the integral closure of $(x,y)R$, a height two ideal. Let P be a height one prime containing x and let S be the integral closure of R/P. Let $f(T) \in R[T]$ be the monic irreducible polynomial satisfied by z. Let $\overline{f}(T) \in S[T]$ be the image of $f(T)$ and let $g(T) = y^{-n}\overline{f}(yT)$ with $n = \deg(f(T))$. Then $g(T) \in S[T]$. Further, if $z \in (x,y)R^+$ and, modulo*

the maximal ideal, $\overline{g}(T) \in K[T]$, then $g(T)$ is a power of a single irreducible factor.

Lemma 4.3. *Let R be a local ring which is a unique factorization domain and p a prime which is the characteristic of the residue field of R. Let S be the integral closure of $R[z]$ where $z^n \in R$, n is prime, and either $p \mid z^n$ or $p \neq n$. Then if $q^n \not\mid z^n$ for all nonunits $q \in R$, it follows that $S = R \oplus Rz \oplus L$ for some L.*

Proof. Let K be the quotient field of R and let $\alpha \in S$. Then $\alpha = a_0 + a_1 z + \cdots + a_{n-1} z^{n-1}$ for some $a_0, \ldots, a_{n-1} \in K$. We wish to show that $a_0, a_1 \in R$. Let q be any prime element of R and define a valuation v' of K by letting $v'(r)$ be the highest power of q dividing r for $0 \neq r \in R$. [Thus $R_{(q)}$ is the valuation ring.] By Theorem 2.8, there exists an extension v of v' to the quotient field of $R[z]$.

First suppose that $v'(z^n) = k$, where $1 \leq k < n$. Then $v(z) = k/n$. Now,

$$v(\alpha) \geq \min_{0 \leq j \leq n-1} \{v(a_j z^j)\} = \min_{0 \leq j \leq n-1} \{jk/n + v(a_j)\},$$

and equality holds if there is a unique minimum. If $jk/n - ik/n$ is an integer, then n must divide $(j-i)k$ which is impossible for n prime. Thus we see that a unique minimum exists and so $v(\alpha) = \min_{0 \leq j \leq n-1} \{jk/n + v(a_j)\}$.

Since α is integral over $R[z]$, we know that $\alpha^n = r_1\alpha^{n-1} + \cdots + r_n$ for some $r_1, \ldots, r_n \in R$. Thus,

$$\begin{array}{rll} & nv(\alpha) & \geq \min_{1\leq i\leq n}\{v(r_i) + (n-i)v(\alpha)\} \\ \Longrightarrow & nv(\alpha) & \geq v(r_i) + (n-i)v(\alpha), \quad \text{for some i} \\ \Longrightarrow & v(\alpha) & \geq v(r_i)/i. \end{array}$$

Hence $v(\alpha) \geq 0$. Since $v(\alpha) = \min_{0\leq j\leq n-1}\{jk/n + v(a_j)\}$, it follows that $v(a_j) \geq -jk/n$ for all j. Hence $v(a_0) \geq 0$ and $v(a_1) \geq -\lfloor k/n \rfloor = 0$.

Next suppose that $v'(z^n) = 0$ and hence $v(z) = 0$. Since we know $\Delta a_i \in R$ for all i where Δ denotes the discriminant of the polynomial $T^n - z^n$ [noting that $\Delta \in R$], we must have $0 \leq v(\Delta a_i) = v(\Delta) + v(a_i)$. The roots of $T^n - z^n$ are $\sigma_1 z, \sigma_2 z, \ldots, \sigma_n z$, where $\sigma_1, \ldots, \sigma_n$ are the roots of $T^n - 1$. Then

$$\begin{aligned} \Delta &= \prod_{i,j}(\sigma_i z - \sigma_j z)^2 \\ &= \prod_{i,j}[z(\sigma_i - \sigma_j)]^2 \\ &= z^{n(n-1)}\prod_{i,j}(\sigma_i - \sigma_j)^2. \end{aligned}$$

So if q divides Δ, we must have $q \mid \Delta_1$ where Δ_1 denotes the discriminant of $f(T) = T^n - 1$. This implies that $f(T)$ has a double root, say σ_i, over $R/(q)$. This would imply that σ_i is also a root of $f'(T) = nT^{n-1}$ modulo q and thus that $n = 0$ in $R/(q)$. But n is a prime number either different from p, and hence a unit in R, or equal to p and dividing z^n. But if $n \mid z^n$, then since $q \nmid z^n$, we can't have $n \in (q)R$. Hence $v(\Delta) = 0$ and so $v(a_i) \geq 0$ for each i.

We have now shown that $a_0, a_1 \in R_{(q)}$ for all prime elements $q \in R$. Thus $a_0, a_1 \in R$, as desired. $\square$

Lemma 4.4. *Let R be a local ring with maximal ideal I which is a unique factorization domain. Suppose n, p are primes with $p \in I$. Let S be the integral closure of $R[z]$ where $z^n \in R$ and either $p \neq n$ or $p \mid z^n$. Then $z \in IS \Leftrightarrow z^n \in t^n R$ for some element $t \in IR$.*

Proof. The reverse implication is obvious since $z/t \in S$. For the forward implication, note that R is a unique factorization domain and if $z^n \notin t^n R$ for any such t, then by Lemma 4.3, $S = R \oplus Rz \oplus L$, for some L. It quickly follows that $z \notin (x, y)S$. □

Proposition 4.5. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x, y)R$ and suppose $p > 3$ is prime with $p \in I$. If $z^3 \in R$ and $z \in IR^+$, then either $z^3 \in I^4$ or $z^3 \in t^3 R$ for some element $t \in (x, y)R$.*

Proof. We shall assume $z \in IR^+$, $z^3 \notin I^4$, and $z^3 \notin t^3 R$ for any element $t \in (x, y)R$ and derive a contradiction. As $z^3 \in I^3$ by (4.1), we may write

$$z^3 = Ax^3 + Bx^2y + Cxy^2 + Dy^3$$

where at least one of the coefficients is a unit. Using a linear change of variable if necessary, we may assume D is a unit. If D is not a cube in R, we may replace R by $R[d]$, where $d^3 = D$ without affecting our hypotheses or assumptions. If $z \in R[d]$ then $z \in IR^+ \cap R[d] = IR[d]$ since the rings are regular local. But then $z = t(r_0 + r_1 d + r_2 d^2)$ which implies that $z^3 \in t^3 R[d]$. Hence the irreducible

polynomial satisfied by z is $f(T) = T^3 - z^3$. Applying Lemma 4.2, we have $g(T) = T^3 - D$ and we can conclude that $T^3 - D = (T - d)(T^2 + dT + d^2)$ is a power of a single irreducible polynomial. This is clearly false for $p \neq 3$. □

Lemma 4.6. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x, y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. If $z^3 - vx^2y^2 \in I^5$ where v is a unit, then $z \notin IR^+$.*

Proof. We assume that $z \in IR^+$, say with $z = \alpha x + \beta y$, and obtain a contradiction. First we claim that either $z^3 \in xR$ or $z^3 \in yR$. Let $S_0 = R[u, s]$ where $u^3 = x$ and $s^3 = y$. Then $z^3 - vs^6u^6 \in (u^3, s^3)^5 S_0$, so $z^3 \in (s^2, u^2)^6 S_0$. In fact, letting $n = p^2$, we have $z^{n-1} - F(s^2)^{n-1}(u^2)^{n-1} \in (s^{2n}, u^{2n})S_0$ where $F = v^{(n-1)/3}$ is a unit. Thus we may apply Corollary 3.6, with $c = d = e = 1$ and $f = 6$. We then obtain elements $a, b \in R^+$ such that $z = s^2a + u^2b$ and b satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral extension of S_0. In addition, modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n - 1$, $a_{n-1} \equiv -Fs^{2(n-1)}$, and $a_n \equiv r$, for some $r \in S_0$. Since z is also equal to $\alpha s^3 + \beta u^3$ it is easily seen that this implies that $b \in (s^2, u)R^+$. We will apply (4.2) to the element b with u in place of x and s^2 in place of y.

Let S denote the integral closure of $S_1[z]$. Suppose that $f(T)$ is irreducible over S. Let P be a height one prime of S containing u. Working modulo P we have $\overline{f}(T) = T^n - \overline{Fs^{2(n-1)}}T + \overline{r}$. By (4.2), the element $\alpha = \overline{r/s^{2n}}$ is integral over S/P. Hence α is in the integral closure of S_0/uS_0. Now S_0/uS_0

is isomorphic to a degree three extension of R/xR. Since no inseparability is possible in a degree three extension, the integral closure of S_0/uS_0 has the same residue field as R since that residue field is separably closed. As in (4.2), we let $g(T) = s^{-2n}\overline{f}(s^2T)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$, and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts (4.2), so our assumption that f is irreducible over S must be false. However, the minimal polynomial for b over S must divide f and using it we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $b \in S$.

Now we have $z \in (s,u)\overline{S_1[z]}$. Then by (4.4), z^3 is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, this implies that $z^3 \in qR$ for some height one prime q which ramifies under the extension to S_1. By Corollary 3.6 the only possibilities are $z^3 \in xR$ or $z^3 \in yR$, and the first claim in proved. Without loss of generality, we may assume then that $z^3 \in yR$.

In a similar manner we now show that either $z^3 - vx^2y^2 \in xyI^3$, or $z^3 - vx^2y^2 \in y^2I^3$. Let $\tilde{z} = z/s$. Then $s\tilde{z} \in (u^3, s^3)R^+$ which implies that $\tilde{z} \in (u^3, s^2)R^+$. Also, $\tilde{z}^3 - vu^6s^3 \in (s^3, u^3)^4S_1$ which implies that $\tilde{z}^3 \in (u^2, s^3)^4$. Letting $n = p^2$, note also that $\tilde{z}^{n-1} - F(u^2)^{n-1}s^{n-1} \in ((u^2)^n, s^n)$ where $F = v^{(n-1)/3}$ is a unit. Thus we may now apply Corollary 3.6 with u^2 in place of x, s in place of y, $c = 3$, $d = e = 1$, and $f = 4$. We obtain $\tilde{z} = u^2a + sb$ where $a, b \in R^+$ and a satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral

extension of S_0. Modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n-1$ and $a_{n-1} \equiv -Fs^{n-1}$. Since $\tilde{z} \in (u^3, s^2)R^+$, it is easily seen that $a \in (u,s)R^+$. Applying (4.2) to the element a gives a contradiction just as above, unless $a \in \overline{S_1[z]}$. But this gives $\tilde{z} \in (s,u)\overline{S_1[\tilde{z}]}$. Then by (4.4), $\tilde{z}^3$ is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, as before this implies that $\tilde{z}^3 \in xR$ or $\tilde{z}^3 \in yR$, as desired.

If $z^3 - vx^2y^2 \in y^2I^3$, let $\tilde{z} = z/s^2$. Then $\tilde{z}^3 - vx^2 \in (x, s^3)^3$. Since $s^2\tilde{z} = z \in (s^3, x)R^+$, we obtain $\tilde{z} \in (x,s)R^+$. But then we must have $x^2 \in (x,s)^3R^+$, which clearly is not true.

If $z^3 - vx^2y^2 \in xyI^3$, let $\tilde{z} = z/su$. Then $\tilde{z}^3 - vs^3u^3 \in (s^3, u^3)^3$. Since $su\tilde{z} = z \in (s^3, u^3)R^+$, we must have $\tilde{z} \in (s^2, u^2)R^+$. But this implies $s^3u^3 \in (s^2, u^2)^3R^+$, also a contradiction. □

Lemma 4.7. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x,y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. If $z \in IR^+$, with $z^3 - vy^2x(y + rx) \in yI^4$ where v is a unit of R and $r \in R$, then $z^3 \in y^3R$ or $z^3 \in xR$.*

Proof. Assume that $z^3 \notin xR$. Let $S_0 = R[u,s]$ where $u^3 = x$ and $s^3 = y$. Let $\tilde{z} = z/s$. Then $s\tilde{z} \in (u^3, s^3)R^+$ which implies that $\tilde{z} \in (u^3, s^2)R^+$ Also we have $\tilde{z}^3 - vs^3u^3(s^3 + ru^3)S_0 \in (s^3, u^3)^4S_0$, which implies that $\tilde{z}^3 \in (s^2, u)^6S_0$. Letting $n = p^2$, note also that $\tilde{z}^{n-1} - F(s^2)^{n-1}u^{n-1} \in ((s^2)^n, u^n)$ where $F = v^{\frac{n-1}{3}}$ is a unit. Thus we may now apply (3.6) with s^2 in place of y, u in place of x,

$c = d = e = 1$, and $f = 6$ to obtain $\tilde{z} = s^2a + ub$ where $a, b \in R^+$ and b satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral extension of S_0. Modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Fs^{2(n-1)}$, and $a_n \equiv r$ for some $r \in S_0$. Since $\tilde{z} \in (u^3, s^2)R^+$, it is easily seen that $b \in (u^2, s^2)R^+$. We will apply (4.2) to the element b with u in place of x and s^2 in place of y.

Let S denote the integral closure of $S_1[\tilde{z}]$. Suppose that $f(T)$ is irreducible over S. Let P be a height one prime of S containing u. Working modulo P we have $\overline{f}(T) = T^n - \overline{Fs^{2(n-1)}}T + \overline{r}$. By (4.2), the element $\alpha = \overline{r/s^{2n}}$ is integral over S/P. Hence α is in the integral closure of S_0/uS_0. Now S_0/uS_0 is isomorphic to a degree three extension of R/xR. Since no inseparability is possible in a degree three extension, the integral closure of S_0/uS_0 has the same residue field as R since that residue field is separably closed. As in (4.2), we let $g(T) = s^{-2n}\overline{f}(s^2T)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$, and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts (4.2), so our assumption that f is irreducible over S must be false. However, the minimal polynomial for b over S must divide f and using it we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $b \in S$. This gives $\tilde{z} \in (s, u)\overline{S_1[\tilde{z}]}$. Then by (4.4), $\tilde{z}^3$ is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, this implies that $\tilde{z}^3 \in qR$ for some height one prime qR which ramifies

under the extension to S_1. By (3.6) since we are assuming that $\tilde{z}^3 \notin xR$ the only possibility is $\tilde{z}^3 \in yR$.

We now have $z^3 - vy^2x(y + rx) \in y^2I^3$. Let $\hat{z} = z/s^2$. Then $s^2\hat{z} \in (u^3, s^3)R^+$ which implies that $\hat{z} \in (u^3, s)R^+$. Also we have, $\hat{z}^3 - vu^3(s^3 + ru^3) \in (s^3, u^3)^3S_0$ which implies that $\hat{z}^3 \in (s^3, u^3)^2S_0$. Letting $n = p^2$, note also that $z^{n-1} - Fs^{n-1}u^{n-1} \in (s^n, u^n)$ where $F = v^{\frac{n-1}{3}}$ is a unit. Thus we may now apply (3.6) with s, u in place of y, x, and with $c = d = 3$, $e = 1$, and $f = 2$ to obtain $\hat{z} = sa + ub$ where $a, b \in R^+$ and b satisfies $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ over S_1, an integral extension of S_0. Modulo the integral closure of a fractional power of u, $a_i \equiv 0$ for $i < n - 1$, $a_{n-1} \equiv -Fs^{n-1}$, and $a_n \equiv r$ for some $r \in S_0$. Since $\hat{z} \in (u^3, s)R^+$, it is easily seen that $b \in (u^2, s)R^+$. Applying (4.2) to the element b gives a contradiction, just as above, unless $b \in \overline{S_1[z]}$. But this gives $\hat{z} \in (s, u)\overline{S_1[\hat{z}]}$. Then by (4.4), $\hat{z}^3$ is a multiple of a cube of an element in the maximal ideal in S_1. Since this was not true in R, and since we are assuming that $\hat{z}^3 \notin xR$, we must have $\hat{z}^3 \in yR$. Thus, $z^3 \in y^3R$. □

Proposition 4.8. *Let R be a Henselian regular local ring of dimension 2 with maximal ideal $I = (x, y)R$ which has a separably closed residue field and suppose $p > 3$ is a prime with $p \in I$. Suppose $z^3 \in R$, $z \in IR^+$, and $z^3 \notin t^3R$ for any element $t \in I$. Then $z^3 \in t^4R + I^5$ for some element $t \in I$.*

Proof. By Proposition 4.5, $z^3 \in I^4$. Suppose that

$$z^3 = Ay^4 + By^3x + Cy^2x^2 + Dyx^3 + Ex^4.$$

We shall first show that either the proposition holds or we can reduce to the special case where $A \in I$ and B is a unit. Later we shall show that the special case leads to a contradiction.

Reducing the coefficients modulo I, we consider the polynomial

$$h(T) = \overline{A}T^4 + \overline{B}T^3 + \overline{C}T^2 + \overline{D}T + \overline{E}.$$

First suppose $\overline{A} = \overline{B} = \overline{C} = \overline{D} = 0$. Then the result holds with $t = x$. So we may assume $h(T)$ is not constant and hence that $h(T)$ is a separable polynomial and so splits over the residue field. We consider five possible cases.

Case 1: Suppose $h(T)$ has a quadruple root. Say $h(T) = \overline{A}(T + r)^4$. Then $z^3 \in t^4R + I^5$ with $t = y + rx$.

Case 2: Suppose $h(T)$ is a polynomial of degree 3. Then we must have $A \in I$ and $B \notin I$ which is the special case.

Case 3: Suppose $h(T)$ is a degree two polynomial and there is a double root. In this case, $A, B \in I$, and $C \notin I$, with $h(T) = \overline{C}(T + r)^2$ for some element r. Then $z^3 - Cx^2(y + rx)^2 \in I^5$. Since $(x, y + rx) = I$, by Lemma 4.6 this is a contradiction.

Case 4: Suppose $h(T)$ is a degree four polynomial and has two double roots. Then it is easily seen that $A \notin I$ and $z^3 - A(y + r_1x)^2(y + r_2x)^2 \in I^5R$, with $r_1 - r_2 \notin I$. Then $I = (y + r_1x, y + r_2x)$ and so (4.6) gives a contradiction.

Case 5: Suppose $h(T)$ has a non-multiple root. This is the only remaining possibility. Call this root r. Let $y' = x$ and $x' = y - rx$. Then we get

$$z^3 = A'(y')^4 + B'(y')^3(x') + \cdots + E'(x')^4.$$

Because r is a root of $h(T)$, $z^3 \in x'R + I^5$. Because r is not a multiple root, $z^3 \notin (x')^2R + I^5$. This tells us that $A' \in I$, and B' must be a unit which is the special case.

Now we have reduced to the special case where $A \in I$, $B \notin I$. Let $S_0 = R[u]$ where $u^3 = x$. Note that S_0 is a regular local ring with maximal ideal $(u, y)S_0$. Suppose first that $z^3 \in xR$. Then $z^* = z/u$ is integral over S_0. As $z \in IR^+$, we have $uz^* \in (y, u^3)R^+$ and so $z^* \in (y, u^2)R^+$. Since $z^3 \in x^2R$ would contradict the assumption that B is a unit we may apply Proposition 4.5 to get $(z^*)^3 \in (y, u)^4S_0 \subset (y^4, u)S_0$. However, this is false as $(z^*)^3$ is congruent to By^3 modulo this last ideal and B is a unit. Thus, $z^3 \notin xR$.

Now we have

$$z^3 = Ay^4 + By^3u^3 + Cy^2u^6 + Dyu^9 + Eu^{12}. \tag{4.1}$$

By changing variables if necessary, we may assume that $z^3 \notin yR$ and still have Equation 4.1 with $A \in I$ and $B \notin I$. Let $n = p^2$. Then

$$z^{n-1} = Fy^{n-1}u^{n-1} + Hu^n + Gy^n,$$

where to compute F, we raise the expression equal to z^3 to the $(n-1)/3$ power and compute the coefficient of $y^{n-1}u^{n-1}$. This is a sum of terms, one of which is $B^{(n-1)/3}$ and the remaining terms are divisible by A. Since $A \in I$,

we see that F is congruent to $B^{(n-1)/3}$ modulo I. Thus we may assume F is a unit. Now we apply Corollary 3.6 with u in place of x, $c = 3$, $d = 1$, and $f = 4$ to find integral elements v, w such that $z = yv + uw$ where w is a root of $f(T) = T^n + a_1T^{n-1} + \cdots + a_n = 0$ over S_1, an integral extension of S_0. As $yv + uw \in (x, y)R^+$, it quickly follows that $uw \in (x, y)R^+ = (u^3, y)R^+$. From there, we see that $w \in (u^2, y)R^+$. We will apply (4.2) with u in place of x.

First, let S denote the integral closure of $S_1[z]$. Suppose that $f(T)$ is irreducible over S. Let P be a height one prime of S containing u. Working modulo P, from the information about the coefficients a_i given in (3.6), we observe that $\overline{f}(T) = T^n - \overline{Fy^{n-1}}T + \overline{r}$, where $r \in S_0$. By (4.2), the element $\alpha = \overline{r/y^n}$ is integral over S/P. Hence α is in the integral closure of S_0/uS_0. Now S_0/uS_0 is isomorphic to R/xR. Hence, the integral closure of S_0/uS_0 has the same residue field as R since that residue field is separably closed. As in (4.2), we let $g(T) = y^{-n}\overline{f}(yT)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$, and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts (4.2), so our assumption that f is irreducible over S must be false. However, the minimal polynomial for w over S must divide f and using it we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $w \in S$.

Since $z = yv + uw$ and S is integrally closed, we obtain $z \in (y, u)S$, so by (4.4), z^3 is a multiple of a cube of some element in the maximal ideal of S. Since this was not the case in R, we must have $z^3 \in xR$ or $z^3 \in yR$ since these

are the only primes containing z^3 which ramify. This contradiction completes the proof.

The next result provides a necessary condition which will be useful in proving (4.12) and (4.15) below.

Proposition 4.9. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Suppose $z^3 \in R$, $z^3 \notin xR$, $z^3 \notin yR$, and $z^3 = \sum_{(i,j)\in S} u_{i,j}y^i x^j$, where each $u_{i,j}$ is a unit of R. Suppose further that there exists $(a, b) \in S$ with $0 \leq a \leq 3$, $4 - a < b < 3(4-a)$, and $\frac{b}{4-a} \leq \frac{j}{4-i}$ whenever $i \leq 3$, $(i, j) \in S$. If there exist $k_1, k_2 \leq p^2-1$ with $bk_1 + (4 - a)k_2 = 4b(\frac{p^2-1}{3})$ such that $z^{p^2-1} - Fy^{k_1}x^{k_2} \in (y^{k_1+1}, x^{k_2+1})$ for some unit F of R, then $z \notin IR^+$.*

Proof. Let $n = p^2$. Let u_1 be an $(n-1)^{\text{st}}$ root of y, u_2 an $(n-1)^{\text{st}}$ root of x, and let $S_0 = R[u_1, u_2]$. Note that S_0 is a Henselian regular local ring with a separably closed residue field and maximal ideal $(u_1, u_2)S_0$. Let $t_i = u_i^{k_i}$. Then $y^{k_1} = t_1^{n-1}$, $x^{k_2} = t_2^{n-1}$ and it follows that $z^{n-1} - Ft_1^{n-1}t_2^{n-1} \in (t_1^n, t_2^n)S_0$.

Let $A = \frac{n-1}{k_1}$ and $B = \frac{n-1}{k_2} \cdot \frac{b}{4-a}$. Then $1/A+1/B = 4/3$ and $p \in (t_1^A, t_2^{Be})$ with $e = \frac{4-a}{b} > \frac{1}{3}$. We may now apply (3.6) provided $z^3 \in (t_1^A, t_2^B)^4$. Since $t_1^A = y$, clearly $y^i x^j \in (t_1^A, t_2^B)^4$ if $i \geq 4$. If $i < 4$ then $\frac{j}{4-i} \geq \frac{b}{4-a}$, or equivalently, $ej \geq (4 - i)$. Hence $y^i x^j = t_1^{Ai} t_2^{Bej} \in (t_1^A, t_2^B)^4$.

We next use (3.6) to get $z = t_1 v + t_2 w$ and a degree n polynomial $f(T)$ satisfied by w. The polynomial $f(T)$ is in $S_1[T]$ for some integral extension

S_1 of S_0. Since $z \in IR^+$, there exists $\alpha, \beta \in R^+$ with $z = y\alpha + x\beta$. Hence $t_2(w - xt_2^{-1}\beta) = t_1(yt_1^{-1}\alpha - v)$. Since t_1 divides y and t_2 divides x and no height one prime contains both t_1 and t_2, $(w - xt_2^{-1}\beta)/t_1 \in R^+$. Thus $w \in (t_1, xt_2^{-1})R^+ \subset (t_1, u_2)R^+$.

Finally we apply (4.2) to the element w with t_1 in place of y and u_2 in place of x. First let S denote the integral closure of $S_1[z]$ and suppose $f(T) = T^n + a_1T^{n-1} + \cdots + a_n$ is irreducible over S. Let P be a height one prime of S containing u_2. From the technical information about $f(T)$ given in (3.6), modulo P we have $a_i \equiv 0$ for $i < n-1$, $a_{n-1} \equiv -Ft_1^{n-1}$, and $a_n \equiv r$ for some $r \in S_0$. Working modulo P we have $\overline{f}(T) = T^n - \overline{Ft_1^{n-1}}T + \overline{r}$. By (4.2), the element $\alpha = \overline{r/t_1^n}$ is integral over S/P. Hence α is in the integral closure of S_0/u_2S_0. Now S_0/u_2S_0 is isomorphic to a degree $n-1$ extension of R/xR. Since R/xR is a discrete valuation ring with maximal ideal generated by y, there is a valuation v on the quotient field of R/xR defined by $v(\alpha y^i) = i(n-1)$ if α is a unit of R/xR. If $v_1^*, \ldots v_k^*$ are the extensions of v to the quotient field of S_0/u_2S_0, then $e_1f_1 + \cdots + e_kf_k \leq n-1$, where f_i and e_i are respectively the relative degree and the reduced ramification index of v_i^* with respect to v. But since $u_1^{n-1} = y$, we must have $v_i^*(u_1) = 1$ and this gives $e_i = n-1$. Hence $k = 1$ and $f_1 = 1$. Thus, the integral closure of S_0/u_2S_0 has the same residue field as R. As in (4.2), we let $g(T) = t_1^{-n}\overline{f}(t_1T)$. Then modulo the maximal ideal of S,

$$\overline{g}(T) = T^n - \overline{F}T + \overline{\alpha}.$$

Hence $\overline{g}(T) \subseteq R/I[T]$, and the derivative is a nonzero constant. Thus, $\overline{g}$ has n distinct roots and therefore must split over R/I. This contradicts (4.2), so our

assumption that f is irreducible over S must be false. However, the minimal polynomial for w over S must divide f and using it we may obtain the same contradiction unless the minimal polynomial is linear. So we have reduced to the case where $w \in S$.

Now we have $z \in (t_1, t_2)S \subset (u_1, u_2)S$. By (4.4), z^3 must be a multiple of the cube of an element in $(u_1, u_2)S_1$. Since this property did not hold in R, and since xR and yR are the only ramified primes in the extension which may contain z^3, we must have $z^3 \in xR$ or $z^3 \in yR$. This contradicts our original assumption.

□

The following lemmas are needed for the proof of Proposition 4.12 below.

Lemma 4.10. *Let p, a, b be integers such that $0 \leq a \leq 3$ and $4-a < b < 3(4-a)$. Use the division algorithm to write $p = 3(4-a)q+r$, with $0 \leq r < 3(4-a)$. If $q + r \geq 3(4 - a)$, then*

$$\frac{p^2-1}{3(4-a)p} \leq \lfloor \frac{p^2-1}{bp} \rfloor.$$

Proof. First, notice that

$$\begin{aligned} \frac{p^2-1}{3(4-a)p} &= \frac{p}{3(4-a)} - \frac{1}{3(4-a)p} \\ &= q + \frac{rp-1}{3(4-a)p}. \end{aligned}$$

So the left hand side is less than $q+1$. Also,

$$\begin{aligned}\lfloor\frac{p^2-1}{bp}\rfloor &\geq \lfloor\frac{p^2-1}{(3(4-a)-1)p}\rfloor \\ &= \lfloor\frac{p}{3(4-a)-1}-\frac{1}{(3(4-a)-1)p}\rfloor \\ &= \lfloor q+\frac{(q+r)p-1}{(3(4-a)-1)p}\rfloor.\end{aligned}$$

So the result holds if $q+r \geq 3(4-a)$. □

Lemma 4.11. *Let a, b be integers such that $0 \leq a \leq 3$ and $4-a < b < 3(4-a)$. Let p be a prime number with $p \geq 29$ and $p \neq 31, 41, 43$. Then with either $k = p\lfloor\frac{p^2-1}{bp}\rfloor$ or $k = \lceil\frac{p^2-1}{3(4-a)}\rceil$, the following must hold:*

(1) $\binom{\frac{p^2-1}{3}}{k}$ *is not divisible by p,*

(2) $k \leq \dfrac{p^2-1}{b}$, *and*

(3) $k \geq \dfrac{p^2-1}{3(4-a)}$.

Proof. For convenience, let $k_1 = p\lfloor\frac{p^2-1}{bp}\rfloor$ and $k_2 = \lceil\frac{p^2-1}{3(4-a)}\rceil$. Notice that (1) holds for k_1 by Lemma 3.7. It's obvious that condition (2) holds for k_1 and that (3) holds for k_2. To see that (2) always holds for k_2, note that unless $a = 1$, $3(4-a)$ divides p^2-1 and certainly $\frac{p^2-1}{3(4-a)} \leq \frac{p^2-1}{b}$. If $a = 1$, then since $b \leq 8$ it suffices to show that $\frac{p^2-1}{9} + 1 \leq \frac{p^2-1}{8}$, or equivalently, that $8(p^2-1) + 72 \leq 9(p^2-1)$. Since $p \geq 29$ this is certainly true.

Use the division algorithm to write $p = 3(4-a)q + r$ with $0 \leq r < 3(4-a)$. By Lemma 4.10, condition (3) holds for k_1 as long as $q+r \geq 3(4-a)$. Hence for $a = 3$ the result is certainly true. If $a = 2$, then $p = 6q + r$, where $r = 1$ or 5 and (3) holds as long as $q + r \geq 6$. Since $q \geq 4$, there is no problem if $r = 5$. If $r = 1$, then indeed $q \geq 5$ since $q = 4$ would give $p = 25$. If $a = 0$ or $a = 1$, we claim that (1) holds for k_2 if $r = 1, 2$, or 5 and that (3) holds for k_1 otherwise. The verification of this claim is enough to complete the proof.

Suppose that $p = 3\lfloor \frac{p}{3} \rfloor + R$. If $r = 1$ or $r = 2$, then $r = R$ and $\lfloor \frac{p}{3} \rfloor = (4-a)q$. If $r = 5$, then $R = 2$ and $\lfloor \frac{p}{3} \rfloor = (4-a)q + 1$. Now, $\frac{p^2-1}{3} = p\lfloor \frac{p}{3} \rfloor + c_0$, where $0 \leq c_0 = \lfloor \frac{p}{3} \rfloor R + \frac{R^2-1}{3} < p$. Similarly, $\frac{p^2-1}{3(4-a)} = pq + a_0$, with $0 \leq a_0 = qr + \frac{r^2-1}{3(4-a)} < p$. Thus, $\frac{p^2-1}{3} - \frac{p^2-1}{3(4-a)} = p(\lfloor \frac{p}{3} \rfloor - q) + c_0 - a_0$. Since $\lfloor \frac{p}{3} \rfloor - q \geq 0$, by (3.7) the first part of the claim holds if $c_0 - a_0 \geq 0$. Since $\lfloor \frac{p}{3} \rfloor \geq q$, certainly $\lfloor \frac{p}{3} \rfloor R + \frac{R^2-1}{3} \geq qr + \frac{r^2-1}{3}$ if $r = R$. Otherwise $r = 5$ and $a_0 = 5q + 8$ while $c_0 = 2\lfloor \frac{p}{3} \rfloor + 1 = 2(4-a)q + 3$. Thus, if $a = 0$, then $q \geq 2$ and so $c_0 = 8q + 3 \geq 5q + 8$ as desired. If $a = 1$, then $q \geq 5$ so $c_0 = 6q + 3 \geq 5q + 8$. So the first part of the claim is true. Now, if $a = 1$, then $p = 9q + r$ with $r \in \{1, 2, 4, 5, 7, 8\}$. If $r = 4$, then (3) holds for k_1 as long as $q \geq 5$. Since q and r must be relatively prime, $q \neq 2, 4$. Since $q = 1$ and $q = 3$ give $p = 13$ and $p = 31$ respectively, and these values of p are not allowed, the result is true if $r = 4$. If $r = 7$, or $r = 8$ then (3) holds for k_1 if $q \geq 2$. Thus the result is true if $a = 1$. Now consider $a = 0$. We have $p = 12q + r$ and if $r \neq 1, 2$, or 5, then we must have $r = 7$, or $r = 11$. For $r = 11$ we see that (3) holds for k_1 as long as $q \geq 1$, which is certainly the case. For $r = 7$, we must check that $q \geq 5$. In fact, it's easy to check that any $q \leq 4$ gives an invalid value for p. □

Theorem 4.12. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let p be a prime integer with $p \in I$, $p \geq 29$, and $p \neq 31, 41, 43$. Suppose z is integral over R with $z^3 \notin yR$ and $z^3 = f(x, y) = y^4A + \sum_{(i,j)\in S} u_{i,j}y^ix^j \in R$, where A and each $u_{i,j}$ are units and the set S satisfies the following:*

(1) *if $(4, j) \in S$, then $j \geq 1$.*

(2) *there is an $(a, b) \in S$ with $0 \leq a \leq 3$ and $4 - a < b < 3(4 - a)$ such that $\frac{b}{4-a} < \frac{j}{4-i}$ whenever $i < 4$, $(i, j) \in S$, $(i, j) \neq (a, b)$.*

Then $z \notin IR^+$.

Proof. Using the construction following Remark 2.1, we may obtain a valuation v on the quotient field of R with $v(y) = b$, $v(x) = 4-a$, and with the valuation of any polynomial in x and y equal to the infimum over all monomials. Then $v(y^4A) = 4b = v(uy^ax^b)$. We claim that $v(z^3) = 4b$ and that only the terms y^4A and uy^ax^b have the minimum value. If $i \geq 4$, then $v(u_{i,j}y^ix^j) = ib + j(4-a) \geq 4b$. In fact, by assumption (1), this value is strictly greater than 4b unless the term is y^4A. If $i < 4$ then $\frac{b}{4-a} < \frac{j}{4-i}$ implies that $b(4-i) < j(4-a)$, or $4b < ib + j(4 - a) = v(u_{i,j}y^ix^j)$, thus proving the claim.

Let $n = p^2$. Let $k = p\lfloor\frac{n-1}{bp}\rfloor$, or $k = \lceil\frac{p^2-1}{3(4-a)}\rceil$ depending on which choice satisfies conditions (1)-(3) of Lemma 4.11. Let $k_1 = 4(\frac{n-1}{3}) - (4 - a)k$, and $k_2 = bk$. Observe that $bk_1 + (4 - a)k_2 = 4b(\frac{n-1}{3})$. By condition (2) of (4.11), $k_2 \leq n - 1$, and by (3), $k_1 \leq n - 1$.

Certainly, we have $z^{n-1} = [f(x,y)]^{\frac{n-1}{3}}$. We first claim that if $y^c x^d$ occurs with unit coefficient in this expression, then either $c \geq k_1 + 1$ or $c + d \geq k_1 + k_2$. If this is not the case, then since $b \geq 4 - a$, we have

$$\begin{aligned} v(y^c x^d) = cb + d(4-a) &\leq k_1 b + (k_2 - 1)(4-a) \\ &\leq 4b(\frac{n-1}{3}) - (4-a). \end{aligned}$$

But we must also have $v(y^c x^d) \geq v(z^{n-1}) = (\frac{n-1}{3})4b$, a contradiction. Thus, $z^{n-1} \subset y^{k_1+1}R + I^{k_1+k_2}$.

Next we claim that there is a term of the form $vy^{k_1}x^{k_2}$ in this expression where v is a unit. In the expansion of $[f(x,y)]^{\frac{n-1}{3}}$ we do in fact have the term $\binom{\frac{n-1}{3}}{k}(y^4 A)^{\frac{n-1}{3}-k}(uy^a x^b)^k = \binom{\frac{n-1}{3}}{k} A^{\frac{n-1}{3}-k} u^k y^{k_1} x^{k_2}$. Since $\binom{\frac{n-1}{3}}{k}$ is a unit by (4.11), we may take $v = \binom{\frac{n-1}{3}}{k} A^{\frac{n-1}{3}-k} u^k$.

Note that the term $vy^{k_1}x^{k_2}$ cannot be cancelled out by terms involving the remaining summands of $f(x,y)$ since $vy^{k_1}x^{k_2}$ has the minimum possible value and all terms with minimal value must come from the binomial expansion of $(Ay^4 + uy^a x^b)^{\frac{n-1}{3}}$. We now have $z^{n-1} - vy^{k_1}x^{k_2} \in (y^{k_1+1}, x^{k_2+1})R$, and an application of (4.9) completes the proof. □

Finally, we would like to point out what remains to be done to complete the proof of Conjecture 1.2 if R is a two dimensional Henselian regular local ring with a separably closed residue field and $I = (x,y)$ is the maximal ideal. We conjecture that if $z \in IR^+$, but $z^3 \notin I^5$, then either $z^3 \in t^3 R$ or $z^3 \in (t, I^3)^4 R$ for some $t \in I$. This is a weaker version of Conjecture 1.2 and seems

to be a key preliminary step to proving that result. By (4.8), we may assume that $z^3 = y^4A + \sum_{(i,j)\in S} u_{i,j}y^ix^j$ with A a unit and $j > 4-i$ for all $(i,j) \in S$. If $i \geq 3$ for all $(i,j) \in S$, then $z^3 \in y^3R$. If $j \geq 3(4-i)$ for every $(i,j) \in S$ then $z^3 \in (y, x^3)^4R$. So by (4.9), to prove this weaker conjecture it remains to prove that $z \notin IR^+$ whenever $z^3 \in yR$ or condition (3) of Proposition 4.12 fails because there is an $(a,b) \in S$ with $0 \leq a \leq 3$ and $4-a < b < 3(4-a)$ such that $\frac{b}{4-a} \leq \frac{j}{4-i}$ whenever $i < 4$, $(i,j) \in S$, and equality holds for at least one $(i,j) \neq (a,b)$. The latter can only happen in the following three situations:

(1) Both $(2,3)$ and $(0,6)$ are in S and $\frac{3}{2} \leq \frac{j}{4-i}$, for $i < 4$.

(2) Both $(2,5)$ and $(0,10)$ are in S and $\frac{5}{2} \leq \frac{j}{4-i}$, for $i < 4$.

(3) Any two of $(3,2), (2,4), (1,6), (0,8)$ are in S and $2 \leq \frac{j}{4-i}$, for $i < 4$.

conjecture it must also be shown are not satisfied.

Our final theorem is a significant step towards resolving the first two of these situations and a good illustration of the tools that we have available. First we need two technical lemmas.

Lemma 4.13. *Let p be a prime and suppose $N = n_1 + n_2 + n_3$ is an integer with $N < p^2$. Using the division algorithm let $N = pq + r$ and $n_i = pq_i + r_i$ for $i = 1,2,3$. Then $p \not| \binom{N}{n_1,n_2,n_3}$ if and only if $q = q_1 + q_2 + q_3$.*

Proof. Let m be an integer. A well-known result from number theory states that the largest k for which $p^k \mid m!$ is precisely

$$k = \lfloor \frac{m}{p} \rfloor + \lfloor \frac{m}{p^2} \rfloor + \cdots$$

Therefore the largest power of p dividing $N!$ is

$$\lfloor \frac{N}{p} \rfloor + \lfloor \frac{N}{p^2} \rfloor + \cdots$$

Since $N < p^2$, this sum reduces to

$$\lfloor \frac{N}{p} \rfloor = \lfloor \frac{pq+r}{p} \rfloor = \lfloor q + \frac{r}{p} \rfloor = q.$$

Similarly, the highest power of p dividing $n_i!$ is q_i. Thus the highest power of p dividing the numerator of $\frac{N!}{n_1!n_2!n_3!}$ is q and the highest power of p dividing the denominator is $q_1 + q_2 + q_3$ so there are two possibilities to consider. If $q = q_1+q_2+q_3$ then $p \not| \binom{N}{n_1,n_2,n_3}$ whereas if $q > q_1+q_2+q_3$ then $p \mid \binom{N}{n_1,n_2,n_3}$. □

Lemma 4.14. *Let $p \equiv 1 \pmod 3$. Let $k = pl$, where $\lfloor \frac{p}{3} \rfloor \leq l \leq \lfloor \frac{p}{2} \rfloor$. Then, letting n denote p^2, $\binom{\frac{n-1}{3}}{i,k-2i,\frac{n-1}{3}-k+i}$ is not divisible by p if and only if $i = pj$ with $l - \lfloor \frac{p}{3} \rfloor \leq j \leq \lfloor \frac{l}{2} \rfloor$. In addition, for such an i,*

$$\binom{\frac{n-1}{3}}{i, k-2i, \frac{n-1}{3}-k+i} \equiv \binom{\lfloor \frac{p}{3} \rfloor}{j, l-2j, \lfloor \frac{p}{3} \rfloor - l + j},$$

modulo p.

Proof. Observe that $p = 3q+1$, where $q = \lfloor \frac{p}{3} \rfloor < p$. Then $n - 1 = 9q^2 + 6q = 3(3q^2 + 2q) = 3(pq + q)$. Hence $\frac{n-1}{3} = pq + q$. Use the division algorithm to write $i = pj + j_0$ with $0 \leq j_0 < p$. Then

$$\frac{n-1}{3} - k + i = p(q - l + j) + (q + j_0).$$

First suppose that $0 \leq q + j_0 < p$. Suppose that $k - 2i = pQ + R$, with $0 \leq R < p$. Then by Lemma 4.13 this binomial coefficient is not divisible by p precisely when $j + Q + (q - l + j) = q$, which gives $Q = l - 2j$. Since $k - 2i = p(l - 2j) - 2j_0$, this happens precisely when $j_0 = 0$.

Now suppose $p \leq q + j_0 < 2p$ (hence $j_0 \geq p - q > 0$), the only remaining possibility. Again, say $k - 2i = pQ + R$ and notice that

$$\frac{n-1}{3} - k + i = p(q - l + j + 1) + (q + j_0 - p)$$

with $0 \leq q + j_0 - p < p$. Applying (4.13) in this case shows that the binomial coefficient is not divisible by p if and only if $Q = l - 2j - 1$. This would give

$$k - 2i = p(l - 2j) - 2j_0 = p(l - 2j - 1) + R,$$

which in turn gives $R = p - 2j_0$. Since $R \geq 0$ we obtain $\frac{p}{2} \geq j_0 \geq p - q$. But this is impossible for $q = \lfloor \frac{p}{3} \rfloor$.

To prove the second statement, we first claim that for any integer of the form $pq + r$ with $q < p$ and $0 \leq r < p$,

$$\frac{(pq + r)!}{p^q} \equiv [(p-1)!]^q q! r!,$$

modulo p. To see this, observe that

$$(pq + r)! = \left[\prod_{y=1}^{r}(pq + y)\right]\left[\prod_{x=0}^{q-1}\prod_{y=1}^{p-1}(px + y)\right]\left[\prod_{x=1}^{q}(px)\right],$$

and the first term is congruent to $r!$, the second is congruent to $[(p-1)!]^q$, and the third equals $p^q q!$.

We saw above that $\frac{n-1}{3} = pq + q$, where $q = \lfloor \frac{p}{3} \rfloor < p$. We also have $i = pj$, $k - 2i = p(l - 2j)$, and $\frac{n-1}{3} - k + i = p(q - l + j) + q$. Since

$j + (l - 2j) + (q - l + j) = q$, the above claim yields

$$\frac{(\frac{n-1}{3})!}{(i)!(k-2i)!(\frac{n-1}{3} - k + i)!} \equiv \frac{q!q!}{j!(l-2j)!(q-l+j)!q!},$$

which is the desired result. □

Proposition 4.15. *Let R be a Henselian regular local ring of dimension two with separably closed residue field and maximal ideal $I = (x, y)R$. Let p be a prime integer with $p \in I$ and $p \equiv 1 \pmod 3$. Suppose z is integral over R with $z^3 = y^4A + y^2x^bB + x^{2b}C + \sum_{(i,j)\in S} u_{i,j}y^ix^j \in R$, where A, B, C are units of R, $3 \leq b \leq 5$, and $\frac{b}{2} < \frac{j}{4-i}$ for every $(i, j) \in S$, $i < 4$. Let*

$$f_l(T) = \sum_{i=l-\lfloor \frac{p}{3} \rfloor}^{\lfloor \frac{p}{2} \rfloor} \binom{\lfloor \frac{p}{3} \rfloor}{i, l-2i, \lfloor \frac{p}{3} \rfloor - l + i} T^i.$$

If AC/B^2 is not a root of $f_l(T)$ modulo the maximal ideal of R for some $\frac{2b-3}{bp}(\frac{p^2-1}{3}) \leq l \leq \lfloor \frac{p}{2} \rfloor$, then $z \notin IR^+$.

Proof. Using the construction following Remark 2.1, we may obtain a valuation v on the quotient field of R with $v(y) = b$, $v(x) = 2$, and with the valuation of any polynomial in x and y equal to the infimum over all monomials. Then $v(y^4A) = v(y^2x^bB) = v(x^{2b}C) = 4b$. We claim that $v(z^3) = 4b$ and that only the terms y^4A, y^2x^bB, and $x^{2b}C$ have the minimum value. If $i < 4$ then $\frac{b}{2} < \frac{j}{4-i}$ implies that $b(4-i) < 2j$, or $4b < bi + 2j = v(y^ix^j)$, thus proving the claim.

Let $n = p^2$ and choose $\frac{2b-3}{bp}(\frac{p^2-1}{3}) \leq l \leq \lfloor \frac{p}{2} \rfloor$. Then l is certainly at least $\lfloor \frac{p}{3} \rfloor$. Let $k = pl$, $k_1 = 2k$, and $k_2 = 2b(\frac{n-1}{3}) - bk$. Then $bk_1 + 2k_2 = 4b(\frac{n-1}{3})$ and $0 \leq k_1, k_2 \leq n-1$. Certainly $z^{n-1} = [y^4 A + y^2 x^b B + x^{2b} C + \sum_{(i,j)\in S} u_{i,j} y^i x^j]^{\frac{n-1}{3}}$. We first claim that if $y^c x^d$ occurs with unit coefficient in this expression, then either $c \geq k_1 + 1$ or $c + d \geq k_1 + k_2$. If this is not the case, then

$$\begin{aligned} v(y^c x^d) = bc + 2d &\leq (b-2)k_1 + 2(k_1 + k_2 - 1) \\ &= bk_1 + 2k_2 - 2 \\ &= 4b(\frac{n-1}{3}) - 2. \end{aligned}$$

But we must also have $v(y^c x^d) \geq v(z^{n-1}) = (\frac{n-1}{3})4b$, a contradiction. Thus, $z^{n-1} - F y^{k_1} x^{k_2} \subseteq (y^{k_1+1}, x^{k_2+1})$, for some $F \in R$. We claim that F is a unit if $f_l(AC/B^2)$ is not congruent to zero modulo the maximal ideal of R. Since $v(y^{k_1} x^{k_2}) = bk_1 + 2k_2 = 4b(\frac{n-1}{3})$ which is the minimum possible value for a term in the expansion of z^{n-1}, the only possible terms contributing to F are those of the form

$$\binom{\frac{n-1}{3}}{i,\, k-2i,\, \frac{n-1}{3} - k + i} A^i B^{k-2i} C^{\frac{n-1}{3} - k + i} y^{2k} x^{2b(\frac{n-1}{3}) - bk},$$

or equivalently,

$$B^k C^{\frac{n-1}{3} - k} \left[\binom{\frac{n-1}{3}}{i,\, k-2i,\, \frac{n-1}{3} - k + i} (\frac{AC}{B^2})^i y^{k_1} x^{k_2} \right],$$

where the binomial coefficient is a unit. Thus by Lemma 4.14 we may take F to be

$$B^k C^{\frac{n-1}{3} - k} \left[\sum_{j = l - \lfloor \frac{p}{3} \rfloor}^{\lfloor \frac{p}{2} \rfloor} \binom{\frac{n-1}{3}}{pj,\, k-2(pj),\, \frac{n-1}{3} - k + pj} (\frac{AC}{B^2})^{pj} \right].$$

By Fermat's Little Theorem $(\frac{AC}{B^2})^{pj} = (\frac{AC}{B^2})^j$. Modulo the maximal ideal, Lemma 4.14 now gives

$$\begin{aligned} F &\equiv B^k C^{\frac{n-1}{3}-k} \left[\sum_{j=l-\lfloor \frac{p}{3} \rfloor}^{\lfloor \frac{p}{2} \rfloor} \binom{\lfloor \frac{p}{3} \rfloor}{j, l-2j, \lfloor \frac{p}{3} \rfloor - l + j} (\frac{AC}{B^2})^j \right] \\ &\equiv B^k C^{\frac{n-1}{3}-k} f_l(\frac{AC}{B^2}), \end{aligned}$$

thus proving the claim. The fact that $z \notin IR^+$ now follows from (4.9). □

Bibliography

[1] R. Heitmann, *The plus closure in mixed characteristic*, J. Algebra **193** (1997), 688-708

[2] R. Heitmann, *The plus closure in degree two extensions*, J. Algebra **218** (1999), 621-641

[3] M. Hochster and C. Huneke, *Tight closure, invariant theory, and the Briançon-Skoda theorem*, J. Amer. Math. Soc. **3** (1990), 31-116

[4] S. Lang, *Algebra*, Addison-Wesley, Menlo Park, CA, 1993

[5] O. Zariski and P. Samuel, *Commutative Algebra, Vol. II*, Van Nostrand, Princeton, NJ, 1958-60

Vita

Leslie Danielle Hayes was born in Ludington, Michigan on July 21, 1973, the daughter of Ronald Lee Hayes and Pamela Dawn Hayes. She has an elder sister, Lynnae, and a younger sister, Lisann. She received the degrees of Bachelor of Arts from Western Michigan University in 1994 and Master of Arts from Washington University in St. Louis in 1997. In September 1998, she entered the Graduate School of the University of Texas at Austin. In the fall of 2001, Ms. Hayes will begin a tenure-track position as Assistant Professor of Mathematics at St. Joseph's University in Philadelphia.

Permanent address: 248 South 23rd Street, Apartment 3F
Philadelphia, PA 19103

This dissertation was typeset with LaTeX[‡] by the author.

[‡]LaTeX is a document preparation system developed by Leslie Lamport as a special version of Donald Knuth's TeX Program.